

Research
IP

Manuel d'utilisation

IPR-TR361

IPR-M1

IPR-TR362

IPR-M2

IPR-TR364

version 3.2

Raritan Computer Inc.

400 Cottontail Lane
Somerset, NJ 08873
United States
Tel. 732-764-8886
Fax 732-764-8887
E-mail : sales@raritan.com
<http://www.raritan.com>

Raritan Computer Europe, B.V.

Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. 31-10-284-4040
Fax 31-10-284-4049
E-mail : sales.europe@raritan.com
<http://www.raritan.com>

Raritan Computer Japan, Inc.

4th Flr. Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku
Tokyo 104-0033
Japan
Tel. 81-03-3523-5991
Fax 81-03-3523-5992
E-mail : sales@raritan.co.jp
<http://www.raritan.co.jp>

Raritan Computer Taiwan, Inc.

5F, 121, Lane 235,
Pao-Chiao Rd., Hsin Tien
Taipei Hsien
Taiwan, ROC
Tel. 886-2-8919-1333
Fax 886-2-8919-1338
E-mail : sales.asia@raritan.com
<http://www.raritan.com.tw>

Raritan Computer France

120 rue Jean Jaurès
93200 Levallois-Perret
France
Tel. 33-14-756-2039
Fax 33-14-756-2061
E-mail : sales.france@raritan.com
<http://www.raritan.fr>

Raritan Computer Deutschland GmbH

Lichtstraße 2
D-45127 Essen
Germany
Tel. 49-201-747-9820
Fax 49-201-747-9850
E-mail : sales.germany@raritan.com
<http://www.raritan.de>



Copyright ©2004 Raritan Computer, Inc.

IPR-01-F

June 2004

255-80-3104

Raritan Computer U.K. Ltd.

36 Great St. Helen's
London
EC3A 6AP
United Kingdom
Tel. 44 20 7614 7700
Fax 44 20 7614 7701
E-mail : sales.uk@raritan.com
<http://www.raritan.com>

**Shanghai Representative Office of
Raritan Computer, Inc.**

RM 19C-1 Shanghai Shiye Building
18 Caoxi North Road
Shanghai China 2000030
Tel. 86-21-64680475
Fax 86-21-64627964
E-mail : sales.asia@raritan.com
<http://www.raritan.com.tw>

Informations FCC

Cet équipement a été testé et certifié conforme aux limites d'un dispositif numérique de classe A selon la section 15 de la réglementation de la Commission fédérale des communications des Etats-Unis (FCC). Ces limites visent à fournir une protection raisonnable contre les interférences nuisibles dans une installation commerciale. Cet équipement génère, utilise et peut émettre des émissions radioélectriques. S'il n'est pas installé et utilisé conformément aux instructions, il risque d'entraîner des interférences perturbant les communications radio. Le fonctionnement de l'équipement dans un environnement résidentiel peut générer des interférences nuisibles.

Marques

Les noms de produits mentionnés dans ce document sont des marques, déposées ou non, de leurs sociétés respectives. IP-Reach, Paragon, MasterConsole MX⁴, MasterConsole II, MasterConsole et leurs logos respectifs sont des marques, déposées ou non, de Raritan Computer, Inc. PS/2, RS/6000 et PC/AT sont des marques déposées de International Business Machines Corporation. Sun est une marque déposée de Sun Microsystems. Microsoft et Windows sont des marques déposées de Microsoft Corporation. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.

Approbations au Japon

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Pour toute assistance aux Etats-Unis, veuillez contacter l'équipe de support technique Raritan par téléphone, au (732) 764-8886, par fax, au (732) 764-8887, ou par courrier électronique, à l'adresse suivante : tech@raritan.com.

Demandez une assistance technique - Du lundi au vendredi, de 8h00 à 20h00 (heure de la côte Est des Etats-Unis).

Pour toute assistance en dehors des Etats-Unis, prenez contact avec le bureau régional Raritan.

Cette page a été laissée vierge intentionnellement.

Table des matières

Chapitre 1 : Introduction	1
Présentation de IP-Reach	1
Accès via Internet, le réseau local/étendu ou un modem d'accès à distance	1
Photos du produit	2
Contenu du coffret	2
Caractéristiques du produit	3
Terminologie	4
Différences entre les modèles	4
Chapitre 2 : Installation	5
Configuration des serveurs cible	5
Résolution vidéo des serveurs	5
Paramètres Windows XP	5
Paramètres Windows 2000/ME	5
Paramètres Windows 95/98/NT	5
Paramètres Linux	6
Paramètres Sun Solaris	6
Paramètres Apple Macintosh	7
Configuration des paramètres du pare-feu du réseau	7
Configuration des switch KVM Paragon	7
Connexions physiques TR Series	8
Câble d'alimentation CA	8
Console d'administration locale	8
Port réseau primaire	8
Port réseau secondaire (facultatif)	8
Ports d'entrée KVM	8
Ports de la console d'accès locale/de sortie KVM (facultatifs)	8
Port de la ligne téléphonique (facultatif)	8
Port d'entrée série (facultatif)	9
Connexions physiques M Series	9
Câble d'alimentation CA	9
Console d'administration locale	9
Port réseau	9
Ports d'entrée KVM	9
Ports de la console d'accès locale/de sortie KVM (facultatifs)	10
Port modem dédié (facultatif)	10
Port d'entrée série (facultatif)	10
Configuration initiale	11
Connexion à distance à IP-Reach	13
Lancement de Raritan Remote Client (RRC)	13
Définition d'une connexion	14
Remarque à l'intention des utilisateurs de CommandCenter	14
Chapitre 3 : Raritan Remote Client	15
Activation de Raritan Remote Client (RRC) par l'intermédiaire d'un navigateur Web	15
Paramètres de sécurité	15
Lancement de Raritan Remote Client	15
Suppression de RRC de la mémoire cache du navigateur	16
Facultatif : installation du logiciel Raritan Remote Client	17
Disposition de la fenêtre RRC	18
Navigateur RRC	19
Options du navigateur	20
Création de nouveaux profils	20
Définition d'une nouvelle connexion	22
Fermeture d'une connexion à distance	22
Barre d'outils et raccourcis RRC	23
Barre d'état RRC	24
Contrôle de la console KVM distante	25
Mode souris simple/Mode souris double	26
Mode plein écran	26
Sélection de serveurs avec un switch KVM	27
Macros de clavier	28
Connexion et propriétés vidéo	31
Calibrage des couleurs	34

Contrôle série à distance	35
Connexion physique	35
Connexion à distance	35
Modification des paramètres série	36
Administration à distance du dispositif	36
Menus de configuration.....	36
Mise à niveau de firmware	36
Redémarrage du dispositif	36
Sauvegarde et restauration de la configuration du dispositif	36
Fichiers journaux.....	37
Chapitre 4 : Fonctions d'administration.....	39
Accès aux fonctions d'administration	39
Console d'administration locale	39
Console d'administration distante	40
Navigation dans les menus d'administration	40
Configuration réseau	41
Configuration du chemin	42
Configuration de la sécurité.....	45
Paramètres des performances	47
Authentification à distance : utilisateurs, groupes et autorisations d'accès	48
Présentation.....	48
Relations entre les utilisateurs et les entrées des groupes.....	48
Création ou modification de comptes groupe	49
Attribution des autorisations d'accès aux ports.....	50
Suppression de comptes groupe	51
Création ou modification de comptes utilisateur	51
Suppression de comptes utilisateur	53
Mise en application d'une authentification à distance	54
Introduction	54
Mise en application d'une authentification à distance	54
Paramètres généraux pour l'authentification à distance	56
Heure et date.....	61
Déconnexion des utilisateurs	61
Affichage de l'état d'IP-Reach	62
Redémarrage ou arrêt d'IP-Reach	62
Diagnostics.....	62
Annexe A : Spécifications	63
Connexion à distance.....	63
Logiciel Raritan Remote Client (RRC).....	63
Entrée KVM	63
Spécifications de câblage.....	64
Spécifications des switch KVM.....	64
Spécifications de sortie	64
Annexe B : Fonctions SNMP	65
Annexe C : Foire Aux Questions.....	67
Annexe D : Guide de dépannage	69
Problèmes et solutions proposées	69
Fichier du journal des événements et codes d'erreur à l'écran	75

Informations importantes

Connexion

- Le nom d'utilisateur et le mot de passe par défaut d'IP-Reach pour la connexion sont respectivement <admin> et <raritan>. Si vous vous connectez sous ce nom d'utilisateur et ce mot de passe, vous disposez des droits d'administrateur.
- Les mots de passe sont sensibles à la casse, ils doivent être saisis exactement de la même manière que lors de leur création.
- Le mot de passe par défaut <raritan> doit être saisi uniquement en lettres minuscules.
- Pour garantir la sécurité du système, modifiez le mot de passe par défaut dès que possible.

Adresse IP par défaut

- IP-Reach est livré avec l'adresse IP par défaut suivante : 192.168.0.192.

Firmware

- Ce manuel s'applique au firmware IP-Reach version 3.2 ou supérieure.

TeleReach

- Jusqu'au 31 janvier 2003, la gamme de produits IP-Reach était connue sous le nom de « TeleReach ».

Cette page a été laissée vierge intentionnellement.

Chapitre 1 : Introduction

Présentation de IP-Reach

Toutes nos félicitations, vous venez de faire l'acquisition d'IP-Reach, la solution de pointe en matière d'accès console KVM à distance, basé sur un réseau, à performances élevées et plates-formes multiples. IP-Reach permet à plusieurs utilisateurs d'accéder simultanément, de manière sécurisée et rentable pour la bande passante, aux consoles KVM de vos serveurs, par l'intermédiaire d'un navigateur Web, indépendant de tout logiciel.

IP-Reach se connecte aux ports clavier, vidéo et souris de quatre serveurs ou switch KVM au maximum. Grâce à la puissante technologie de capture d'image et d'algorithme de compression vidéo de Raritan, il capture, numérise et compresse le signal vidéo avant de le transmettre à un ordinateur distant. L'utilisateur distant dispose d'un accès direct et d'un contrôle total des serveurs cible aux fins des opérations de maintenance, d'administration, de dépannage - de l'exécution d'applications via l'interface utilisateur aux interventions de niveau BIOS - et même de redémarrage.

IP-Reach vous permet d'accéder facilement à vos serveurs, n'importe quand, de n'importe où :

- Contrôlez les serveurs situés au sein du bâtiment même ou à l'autre bout du campus.
- Gérez les serveurs des filiales depuis un site centralisé.
- Fournissez une assistance à distance aux centres de données du monde entier.
- Dépannez, reconfigurez et redémarrez les serveurs depuis votre domicile.
- Assurez une gestion des serveurs adaptée et sécurisée en service réduit.

Accès via Internet, le réseau local/étendu ou un modem d'accès à distance

IP-Reach propose une large gamme de méthodes d'accès à distance permettant de contrôler les serveurs connectés à un switch KVM de Raritan. IP-Reach permet également d'accéder aux serveurs hors bande, l'accès distant aux serveurs cible vitaux est donc toujours possible - même lorsque le réseau n'est pas opérationnel.

Photos du produit



IP-Reach M Series



IP-Reach TR Series

Contenu du coffret

L'unité IP-Reach fournie est un produit autonome totalement configuré, monté dans un châssis de montage en rack 2U de 19" standard. Les éléments suivants sont également inclus :

TR Series

- (1) Unité IP-Reach
- (1) Guide d'installation et de configuration rapide d'IP-Reach TR Series
- (1) Manuel d'utilisation d'IP-Reach
- (1) CD-ROM du logiciel Raritan Remote Client
- (1) Kit de montage en rack
- (1) Câble d'alimentation
- (1) Câble téléphonique RJ11
- (N) Câbles coaxiaux CCP20
- (N) Câbles coaxiaux CCP20F

M Series

- (1) Unité IP-Reach
- (1) Guide d'installation et de configuration rapide d'IP-Reach M Series
- (1) Manuel d'utilisation d'IP-Reach
- (1) CD-ROM du logiciel Raritan Remote Client
- (1) Kit de montage en rack
- (1) Câble d'alimentation
- (N) Câbles coaxiaux CCP20

(N = nombre de ports)

Caractéristiques du produit

Accès

- Accès KVM à distance via Internet, le réseau local/étendu ou un modem d'accès à distance
- Connexion de quatre utilisateurs simultanés maximum au(x) switch ou au(x) serveur(s)
- Seize utilisateurs simultanés maximum (utilisation du mode PC-share)
- Accessible via un navigateur Web
- Accès à distance aux dispositifs série (VT100) connectés au port série d'IP-Reach

Performances

- Algorithme de compression de qualité supérieure garantissant des performances hors du commun
- Aucun impact sur les performances des serveurs cible
- Détection automatique de la résolution vidéo permettant d'obtenir un affichage optimal
- Synchronisation et traçage de la souris hautes performances

Fiabilité

- Alimentations à double protection par basculement*
- Ethernet à double protection par basculement*
- Modem intégré*/Port modem dédié** permettant d'accéder aux serveurs même lorsque le réseau n'est pas disponible

Sécurité

- Chiffrement SSL 128 bits RSA à clé publique, chiffrement 128 bits RC4 à clé privée.
- Port TCP configurable unique permettant d'assurer la protection du pare-feu
- Prend en charge les protocoles d'authentification RADIUS et LDAP

Administration

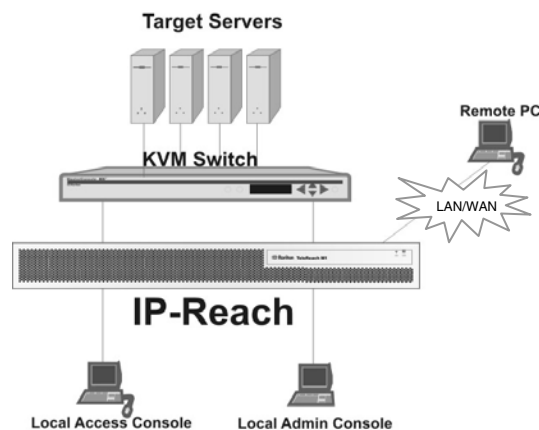
- Administration à distance via l'interface du navigateur Web
- Intégration étroite avec la console de gestion CommandCenter
- Prise en charge SNMP
- Mise à niveau du firmware via Ethernet
- Installation et interface utilisateur simplifiées
- Console utilisateur permettant un accès analogique direct au switch KVM
- Journal des événements utilisateur complet pouvant être téléchargé
- Adressage DHCP ou IP fixe

* IP-Reach TR Series uniquement

** IP-Reach M Series uniquement

Terminologie

Ce manuel utilise les termes suivants pour désigner les composants d'une configuration IP-Reach type. Lors de la lecture de ce manuel, veuillez vous reporter au schéma ci-dessous pour obtenir des explications (si nécessaire).



Serveur(s) cible	Serveurs auxquels vous accédez à distance via IP-Reach et la configuration KVM connectée.
Ordinateur distant	Ordinateur Windows utilisé pour accéder aux serveurs cible connectés à IP-Reach et les contrôler.
Console d'accès locale	Une console utilisateur facultative, composée d'un clavier PS/2, d'une souris PS/2 et d'un écran VGA, directement connectée à IP-Reach afin de contrôler les serveurs cible localement (et non par l'intermédiaire du réseau). Les modèles IP-Reach à un port (IPR-TR361 et IPR-M1) permettent de connecter une console d'accès locale. Les modèles IP-Reach à deux ports (IPR-TR362 et IPR-M2) permettent de connecter deux consoles d'accès locale, les modèles IP-Reach à trois ports permettent de connecter trois consoles, etc.
Console d'administration locale	Un clavier PS/2 et un écran VGA directement connectés à IP-Reach et permettant l'administration et la configuration. Cette console vous permet d'accéder directement aux menus d'administration d'IP-Reach. Il est impossible d'afficher les serveurs cible de la configuration KVM connectée sur cet écran. IP-Reach permet également de réaliser une administration à distance via le réseau. La console d'administration locale constitue cependant le moyen le plus simple de procéder à la configuration initiale.

Différences entre les modèles

Raritan propose deux gammes de modèles IP-Reach : TR Series et M Series. Les deux gammes de modèles présentent les mêmes ensembles de fonctions et le même niveau de performances. Les modèles TR Series disposent néanmoins des avantages matériels suivants, qui répondent aux exigences des applications de classe transporteur :

- Alimentation à double redondance
- Contrôleurs Ethernet à double protection par basculement
- Mise à niveau de la densité de port (jusqu'à quatre ports)
- Modem intégré
- Hauteur de rack 2U

Chapitre 2 : Installation

Configuration des serveurs cible

Avant d'installer IP-Reach, vous devez, afin d'obtenir des performances optimales, configurer les serveurs cible auxquels vous souhaitez accéder via IP-Reach comme indiqué ci-dessous. Notez que la configuration requise suivante s'applique uniquement aux *serveurs cible*, et non aux ordinateurs utilisés pour accéder à distance à IP-Reach (reportez-vous au **Chapitre 1 : Introduction, Terminologie**).

Résolution vidéo des serveurs

Pour une utilisation de bande passante et une qualité vidéo optimales, les serveurs cible exécutant des interfaces utilisateur graphiques telles que Windows, X-Windows, Solaris et KDE, doivent être configurés avec des papiers peints de Bureau définis sur une image uniforme légèrement colorée. Evitez les papiers peints ornés de photos ou de dégradés complexes.

Assurez-vous qu'IP-Reach prend en charge la résolution vidéo et le taux de rafraîchissement du serveur et que le signal est non entrelacé. IP-Reach prend en charge les résolutions vidéo suivantes :

Modes texte

640x480 à 60Hz	1024x768 à 60Hz
640x480 à 72Hz	1024x768 à 70Hz
640x480 à 75Hz	1024x768 à 75Hz
640x480 à 85Hz	1024x768 à 85Hz
800x600 à 56Hz	1152x864 à 60Hz
800x600 à 60Hz	1152x864 à 75Hz
800x600 à 72Hz	1280x1024 à 60Hz
800x600 à 75Hz	
800x600 à 85Hz	

Paramètres Windows XP

Sur les serveurs cible exécutant Microsoft Windows XP, désactivez l'option **Améliorer la précision du pointeur** et définissez la vitesse du pointeur de la souris exactement au milieu. Ces paramètres se trouvent sous **Panneau de configuration → Souris → Pointeurs de souris**.

***Remarque :** pour les serveurs cible exécutant Windows NT, 2000 ou XP, il est possible que vous souhaitiez créer un nom d'utilisateur uniquement utilisé pour les connexions à distance par l'intermédiaire d'IP-Reach. Cette opération vous permet de conserver les paramètres d'accélération/de mouvement lent du pointeur de la souris du serveur cible exclusivement pour la connexion IP-Reach. Il est en effet possible que les autres utilisateurs souhaitent que la souris se déplace plus rapidement.*

***Remarque :** les écrans de connexion de Windows XP et 2000 rétablissent les paramètres prédéfinis de la souris qui diffèrent des paramètres suggérés pour une performance optimale d'IP-Reach. La synchronisation de la souris ne sera donc pas optimale sur ces écrans. Si vous savez comment régler le registre des serveurs cible Windows, vous pouvez obtenir une meilleure synchronisation de la souris IP-Reach sur les écrans de connexion en utilisant l'éditeur de registre Windows pour modifier les paramètres suivants : vitesse par défaut du pointeur de la souris utilisateur = 0, seuil de la souris 1 = 0, seuil de la souris 2 = 0.*

Paramètres Windows 2000/ME

Sur les serveurs cible exécutant Microsoft Windows 2000/ME, réglez l'accélération du pointeur de la souris sur **Aucune** et définissez la vitesse du pointeur de la souris en sélectionnant le paramètre qui se trouve exactement au milieu. Ces paramètres se trouvent sous **Panneau de configuration → Souris**.

Paramètres Windows 95/98/NT

Sur les serveurs cible exécutant Microsoft Windows 95/98/NT, définissez la vitesse du pointeur de la souris en sélectionnant le paramètre le plus faible sous **Panneau de configuration → Souris → Mouvement du pointeur**.

Paramètres Linux

Sur les serveurs cible exécutant des interfaces graphiques Linux, réglez l'accélération de la souris sur 1 exactement et le seuil sur 1 exactement.

Comme indiqué ci-dessus, veuillez vous assurer que tous les serveurs cible exécutant Linux utilisent une résolution VESA standard et un taux de rafraîchissement pris en charge par IP-Reach. Les serveurs cible Linux doivent également être configurés de manière à ce que les temps de passage en blanc correspondent aux valeurs VESA standard +/- 40 %.

Pour vérifier ces paramètres :

- Localisez le fichier de configuration Xfree86 (XF86Config).
- Désactivez toutes les résolutions qui ne sont pas prises en charge par IP-Reach à l'aide d'un éditeur de texte.
- Désactivez la fonction de bureau virtuel (elle n'est pas prise en charge par IP-Reach).
- Vérifiez les temps de passage en blanc (valeurs VESA standard +/- 40 %).
- Redémarrez l'ordinateur.

Remarque : dans de nombreux environnements graphiques Linux, la commande **<Ctrl+Alt+Plus>** modifie la résolution vidéo en parcourant toutes les résolutions disponibles qui restent activées dans le fichier *XF86Config*.

Paramètres Sun Solaris

Tous les serveurs cible doivent utiliser une des résolutions d'affichage prises en charge par IP-Reach. Les résolutions les plus courantes sur les ordinateurs Sun sont :

- 1024 x 768 à 60 Hz
- 1024 x 768 à 70 Hz
- 1024 x 768 à 75 Hz
- 1024 x 768 à 85 Hz
- 1152 x 900 à 66 Hz
- 1152 x 900 à 76 Hz
- 1280 x 1024 à 60 Hz

Les serveurs cible exécutant le système d'exploitation Solaris doivent utiliser une sortie vidéo VGA (signaux H-Sync et V-Sync, pas à synchronisation composite). Pour passer d'une sortie de carte graphique Sun synchronisée de manière composite à une sortie VGA non standard, lancez d'abord la commande **Stop+A** pour afficher le mode bootprom. Puis lancez la commande

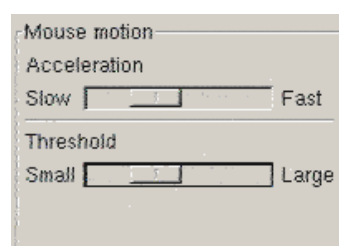
```
setenv output-device screen:r1024x768x70
```

pour modifier la résolution de sortie. Lancez la commande « **boot** » pour redémarrer le serveur.

Vous pouvez également vous procurer un adaptateur de sortie vidéo auprès de votre représentant Raritan. Les ports Sun 13W3 avec une sortie synchronisée de manière composite nécessitent l'utilisation d'un Guardian Raritan APSSUN II avec IP-Reach. Les ports Sun HD15 avec une sortie synchronisée de manière composite nécessitent l'utilisation d'un convertisseur Raritan 1396C pour convertir la sortie vidéo HD15 en sortie 13W3, et d'un convertisseur Guardian Raritan APSSUN II pour prendre en charge la synchronisation composite. Les ports Sun HD15 avec une sortie synchronisée de manière séparée nécessitent l'utilisation d'un Guardian Raritan APKMSUN avec IP-Reach.

Notez qu'il est possible que les switch KVM de marque autre que Raritan ne traite pas correctement les signaux PS/2 vers Sun.

Sur les serveurs cible exécutant un système d'exploitation Solaris, réglez l'accélération de la souris sur 1 exactement et le seuil sur 1 exactement. Effectuez ce réglage au niveau de l'interface utilisateur graphique (illustrée ci-dessous) ou à l'aide de la ligne de commande « **xset mouse a t** », où la lettre « a » correspond à l'accélération et la lettre « t » au seuil.



Paramètres Apple Macintosh

Sur les serveurs cible exécutant un système d'exploitation Apple Macintosh, si vous utilisez IP-Reach pour accéder à votre serveur cible et le contrôler, vous devez régler le client IP-Reach (Raritan Remote Client) sur le mode « curseur simple ». Le mode curseur double n'est pas pris en charge. En outre, si vous tentez de contrôler un serveur Macintosh par l'intermédiaire d'IP-Reach en mode curseur double, les deux pointeurs de la souris ne s'affichent pas de manière synchronisée.

Configuration des paramètres du pare-feu du réseau

Si vous souhaitez accéder à IP-Reach par l'intermédiaire du pare-feu d'un réseau, votre pare-feu doit permettre la communication sur le port TCP 5000. Vous pouvez également configurer IP-Reach pour permettre l'utilisation d'un port TCP de votre choix (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**).

Si vous souhaitez bénéficier des possibilités d'accès Web d'IP-Reach, le pare-feu doit autoriser la communication en amont sur le port TCP 443 (port TCP standard pour la communication HTTPS). Si vous souhaitez qu'IP-Reach redirige automatiquement les requêtes HTTP vers HTTPS (de manière à ce que les utilisateurs utilisent « http://xxx.xx.xxxx », plus courant, à la place de « https://xxx.xx.xxxx »), le pare-feu doit autoriser la communication en amont sur le port TCP 80 (port TCP standard pour la communication HTTP).

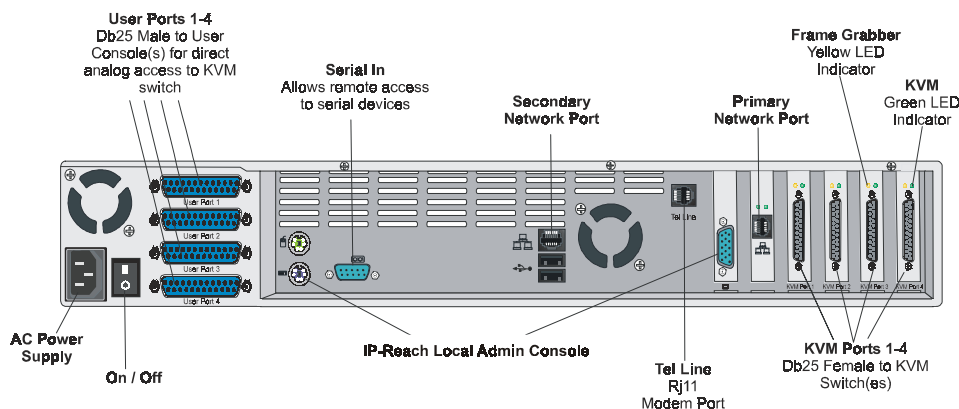
Configuration des switch KVM Paragon

Si vous souhaitez utiliser IP-Reach pour accéder à des switch KVM de classe entreprise Paragon de Raritan, vous devez procéder à l'optimisation suivante avant de connecter IP-Reach :

affichez les serveurs cible accessibles à partir de la station utilisateur Paragon les uns après les autres et réglez le paramètre de la qualité vidéo sur -15 (moins 15). Ajustez la qualité vidéo de Paragon à l'aide de la touche + ou - de votre clavier numérique tout en consultant l'interface utilisateur à l'écran.

Lors du réglage, la ligne inférieure du menu de l'interface utilisateur à l'écran affichera les modifications du paramètre de la qualité vidéo à mesure que vous appuyez sur la touche + ou -. Une qualité vidéo équivalente à -15 permet d'obtenir l'image la plus claire lors de l'affichage des serveurs cible par l'intermédiaire d'IP-Reach, depuis un ordinateur distant. Procédez à ce réglage pour l'ensemble des serveurs cible et des stations utilisateur connectés à IP-Reach.

Connexions physiques TR Series



Panneau arrière de l'unité IP-Reach TR Series

Câble d'alimentation CA

Raccordez le câble d'alimentation CA fourni à l'unité IP-Reach et à une prise CA.

Console d'administration locale

Raccordez un clavier PS/2 et un écran Multisync aux ports indiqués (reportez-vous au schéma ci-dessus), situés sur la partie arrière d'IP-Reach.

Port réseau primaire

Reliez le port réseau à un routeur, un concentrateur ou un switch Ethernet à l'aide d'un câble Ethernet standard.

Port réseau secondaire (facultatif)

Reliez le port réseau à un routeur, un concentrateur ou un switch Ethernet à l'aide d'un câble Ethernet standard. Lorsque le port réseau primaire n'est pas disponible, IP-Reach bascule automatiquement sur le port réseau secondaire. Pour connaître la procédure à suivre pour activer la prise en charge du basculement Ethernet, reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**.

Ports d'entrée KVM

Reliez le port d'entrée KVM à la console KVM du serveur ou du switch KVM auquel vous souhaitez accéder à distance à l'aide du ou des câbles CCP20 fournis.

Ports de la console d'accès locale/de sortie KVM (facultatifs)

Les ports utilisateur de sortie KVM permettent un accès analogique direct au serveur ou au switch KVM relié aux ports d'entrée KVM correspondants. Reliez les ports repérés par la mention « User Port » à un clavier PS/2, une souris PS/2 et un écran VGA Multisync à l'aide du ou des câbles CCP20F inclus.

Remarque : les consoles d'accès locales peuvent être reliées aux ports utilisateur 1 à 4. Les consoles d'accès locales affichent alors le switch KVM ou le serveur relié au port KVM correspondant. La console utilisateur relié au port utilisateur 1, par exemple, affiche le switch KVM ou le serveur relié au port KVM 1. La console utilisateur relié au port utilisateur 2 affiche le switch KVM ou le serveur relié au port KVM 2, etc.

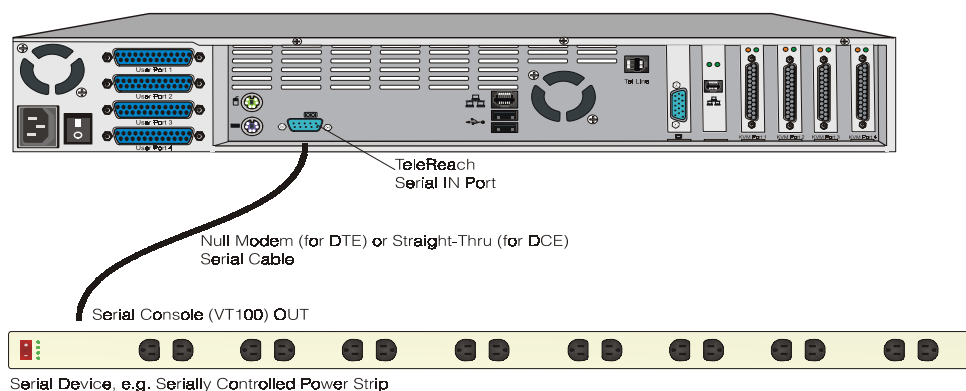
Port de la ligne téléphonique (facultatif)

Les modèles IP-Reach TR Series disposent d'un modem intégré permettant l'accès à distance lorsque le réseau local/étendu n'est pas disponible. Reliez le port repéré par la mention « Tel Line » à une prise téléphonique analogique à l'aide du câble téléphonique fourni.

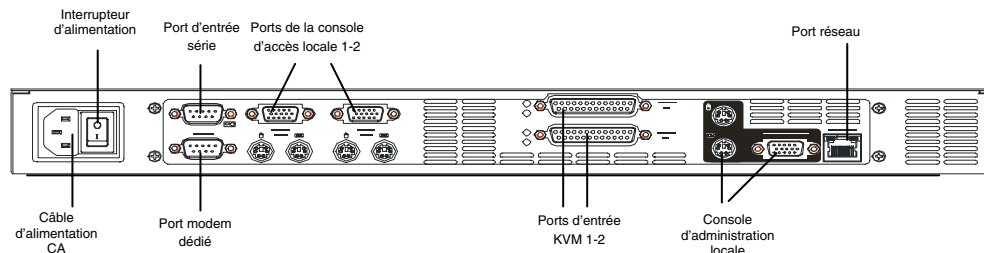
Port d'entrée série (facultatif)

Il est possible d'accéder à distance à des dispositifs contrôlés en série (émulation du terminal VT100) via IP-Reach. Il suffit pour cela de les relier au port d'entrée série, situé sur la partie arrière d'IP-Reach.

Le port série d'IP-Reach est un port de type DTE. Lors de la connexion d'un autre dispositif série DTE à IP-Reach, utilisez un câble série null-modem. Lors de la connexion d'un dispositif série DCE à IP-Reach, utilisez un câble série à brochage direct.



Connexions physiques M Series



Panneau arrière de l'unité IP-Reach M Series

Câble d'alimentation CA

Raccordez le câble d'alimentation CA fourni à l'unité IP-Reach et à une prise CA.

Console d'administration locale

Raccordez un clavier PS/2 et un écran Multisync aux ports correspondants situés sur la partie arrière d'IP-Reach et repérés par la mention « Admin Console ».

Port réseau

Reliez le port réseau à un routeur, un concentrateur ou un switch Ethernet à l'aide d'un câble Ethernet standard.

Ports d'entrée KVM

Connectez l'extrémité DB25 du ou des câbles CCP20 fournis aux ports « KVM » et l'autre extrémité du câble CCP aux ports vidéo VGA, souris et clavier PS/2 des switch KVM ou des serveurs pour lesquels vous souhaitez disposer d'un accès réseau à distance.

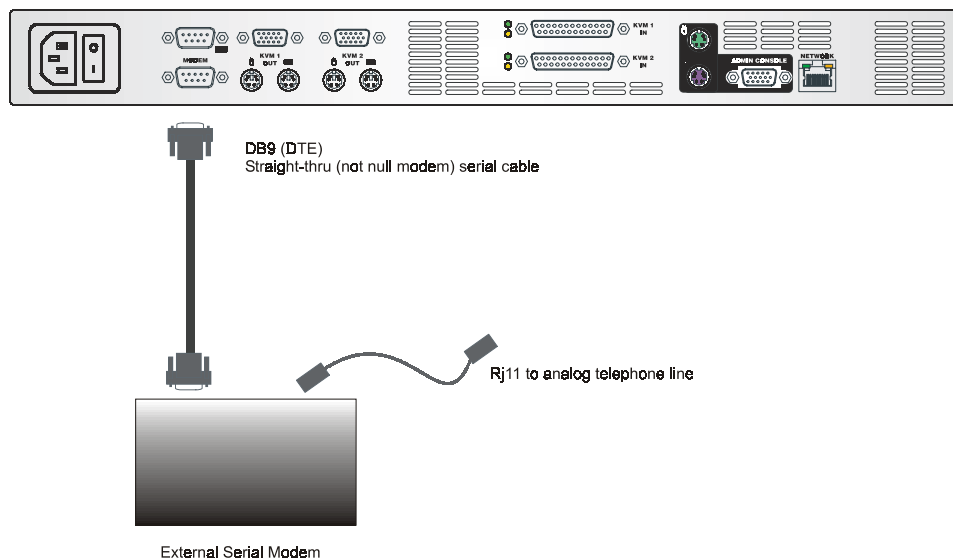
Ports de la console d'accès locale/de sortie KVM (facultatifs)

Connectez un clavier PS/2, une souris et un écran Multisync à ces ports si vous souhaitez disposer d'un accès analogique direct aux serveurs ou aux switch KVM reliés aux ports « KVM In » correspondants.

Remarque : avec le modèle IP-Reach M2, lorsque la console d'accès locale est reliée à un port « KVM Out », elle affiche le switch KVM ou le serveur connecté au numéro de port « KVM In » correspondant. Si la console utilisateur est reliée au port « KVM Out » 1, par exemple, elle affiche le switch KVM ou le serveur connecté au port « KVM In » 1.

Port modem dédié (facultatif)

Les modèles IP-Reach M Series disposent d'un port modem dédié. La connexion d'un modem série externe standard à ce port permet aux utilisateurs de conserver un accès à distance à IP-Reach lorsque le réseau local/étendu n'est pas disponible.



Utilisez un câble série à brochage direct standard pour relier IP-Reach à votre modem série externe. Connectez ensuite le port « Tel Line » de votre modem à une ligne téléphonique analogique (pour plus de détails, reportez-vous à la documentation de votre modem série externe).

Port d'entrée série (facultatif)

Il est possible d'accéder à distance à des dispositifs contrôlés en série (émulation du terminal VT100) via IP-Reach. Il suffit pour cela de les relier au port d'entrée série, situé sur la partie arrière d'IP-Reach.

Le port série d'IP-Reach est un port de type DTE. Lors de la connexion d'un autre dispositif série DTE à IP-Reach, utilisez un câble série null-modem. Lors de la connexion d'un dispositif série DCE à IP-Reach, utilisez un câble série à brochage direct.

Configuration initiale

Lors de la configuration initiale, l'**assistant de configuration IP-Reach** vous aide à procéder rapidement à la première configuration d'IP-Reach. L'assistant de configuration IP-Reach s'affiche uniquement lorsque vous accédez aux menus d'administration sur un IP-Reach non configuré. Il vous guide tout au long du paramétrage de la configuration initiale. Le moyen le plus simple pour procéder à la configuration initiale consiste à utiliser la console d'administration locale (reportez-vous aux instructions de la rubrique « Connexions physiques » dans les sections précédentes).

1. Mettez IP-Reach SOUS tension à l'aide de l'interrupteur d'alimentation situé sur la partie arrière de l'unité IP-Reach.
2. L'écran de bienvenue de l'assistant de configuration IP-Reach s'affiche sur la console d'administration locale.

```

Welcome to IP-Reach

IP-Reach has not been configured. Minimal configuration requirements
to make IP-Reach operational include entry of named-user software key
codes and assignment of an IP address or enabling the modem interface.

Following the IP-Reach Setup Wizard is the simplest way to perform
the configuration requirements needed to start working with IP-Reach.
Additional configuration options may be set at a later time through
the main menu - See Local Administrative Functions in your IP-Reach
User Manual.

Press B to begin the IPReach Setup Wizard.
Press X to bypass the Setup Wizard and proceed to the Main Menu.

```

3. Appuyez sur la lettre du clavier de la console d'administration locale pour lancer l'assistant de configuration IP-Reach.
4. L'écran Network Configuration (Configuration réseau) s'affiche.

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Network Configuration -

Name                                     [IPR-Joel      ]

Enable Ethernet Interface                [YES]
Line Speed & Duplex                     [Auto Detect  ]
Obtain IP address automatically (DHCP)  [NO ]
IP Address                             [192.168. 51.150]
Subnet Mask                             [255.255.255. 0 ]
Default Gateway                         [ 0 . 0 . 0 . 0 ]

Enable Modem Interface                  [NO ]
Enable Web Browser Interface            [YES]
Use Default TCP Port 5000               [YES]

Enable IP Failover                      [NO ]

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

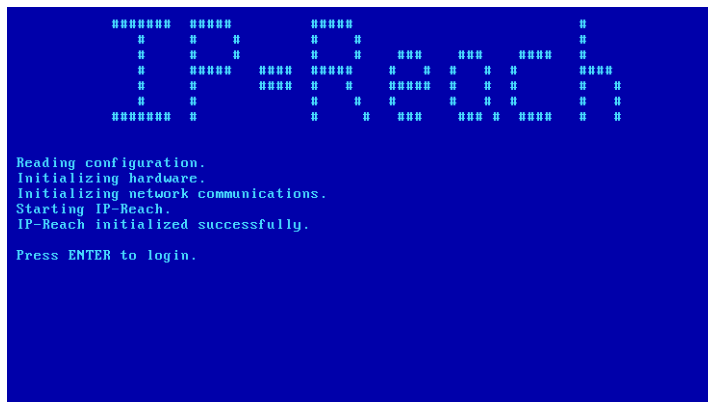
5. Utilisez la touche <Tabulation>, <↑> ou <↓> pour sélectionner les lignes de l'écran Network Configuration (Configuration réseau) et la touche <barre d'espace>, <←> ou <→> pour naviguer entre les entrée disponibles. Une fois la saisie des différentes lignes terminée, appuyez sur la touche <Entrée>, <Tabulation> ou <↓>. Vous trouverez ci-dessous les descriptions relatives à chaque champ ainsi que les valeurs qui doivent être affectées.
 - **Name (Nom)** : indique le nom (unique) de l'unité IP-Reach, « Centre de données de Miami », par exemple. Le nom par défaut est **IP-Reach**.
 - **Enable Ethernet Interface (Activer l'interface Ethernet)** : indique si IP-Reach doit activer son adaptateur Ethernet (valeur par défaut : YES (OUI)).

Remarque : les connexions réseau doivent être de type Ethernet 10BASE-T ou 100BASE-TX.

- **Line Speed & Duplex (Vitesse de ligne & Duplex) :** définissez l'efficacité visuelle de l'écran : Auto detect 10 Mbps/Full Duplex (Détection automatique 10 Mbps/Full Duplex), 10 Mbps/Half Duplex, 100 Mbps/Full Duplex ou 100 Mbps/Half Duplex.
- **Obtain IP address automatically (DHCP) (Obtenir l'adresse IP automatiquement (DHCP)) :**
 - ♦ **YES (OUI) :** l'adressage IP dynamique d'IP-Reach est activé. A chaque redémarrage, IP-Reach demande une adresse IP auprès du serveur DHCP local. Notez que ce paramètre peut rendre l'accès à distance à IP-Reach difficile hors du réseau local. En effet, pour initier une connexion, l'adresse IP affectée de manière dynamique doit être connue.
 - ♦ **NO (NON) (valeur par défaut) :** une adresse IP fixe est attribuée à l'unité IP-Reach (recommandé).
 - **IP Address (Adresse IP) :** saisissez l'adresse IP que votre administrateur réseau vous a donnée pour IP-Reach.
 - **Subnet Mask (Masque de sous-réseau) :** saisissez le masque de sous-réseau fourni par votre administrateur réseau.
 - **Default Gateway (Passerelle par défaut) :** saisissez la passerelle par défaut indiquée par votre administrateur réseau (le cas échéant).
- **Enable Modem Interface (Activer l'interface du modem) :** l'accès via le modem d'accès à distance est activé (valeur par défaut : YES (OUI)). Sur les modèles IP-Reach M Series, il est nécessaire qu'un modem série externe soit connecté pour que le fonctionnement de ce paramètre soit garanti (reportez-vous au **Chapitre 2 : Installation, Connexions physiques M Series, Port modem dédié**).
- **Enable Web Browser Interface (Activer l'interface du navigateur Web) :** l'accès à IP-Reach via le navigateur Web est activé (valeur par défaut : YES (OUI)).
- **Use Default TCP Port 5000 (Utiliser le port TCP 5000 par défaut) :**
 - **YES (OUI) (valeur par défaut) :** le port TCP 5000 par défaut est utilisé.
 - **NO (NON) :** saisissez le numéro du port que vous souhaitez utiliser à la place.

***Remarque :** si vous souhaitez accéder à IP-Reach sans l'aide d'un pare-feu, les paramètres que vous définissez pour le pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut (et non du port personnalisé configuré ci-dessus).*

- **Enable IP Failover (Activer le basculement IP) (modèles TR Series uniquement) :** ce paramètre (uniquement disponible pour les modèles TR Series) permet d'activer le port Ethernet secondaire en cas de défaillance.
 - Lorsque ce paramètre est activé, IP-Reach vérifie la disponibilité de son port Ethernet primaire selon un intervalle constant, indiqué par le paramètre **Ping Interval in seconds (Intervalle ping en secondes)**.
 - Lors des vérifications ping, effectuées à intervalles réguliers, si le port Ethernet n'est pas disponible pendant un délai supérieur à celui indiqué par le paramètre **Failover Timeout in seconds (Délai de défaillance en secondes)**, IP-Reach désactive automatiquement son port Ethernet primaire et active son port Ethernet secondaire.
6. Appuyez sur <Ctrl+S> pour enregistrer les éléments que vous avez saisis. Le menu principal s'affiche.
 7. Dans le menu principal, sélectionnez [R] **Restart or shutdown the IP-Reach (Redémarrer ou éteindre IP-Reach)** et appuyez sur la touche <Entrée>.
 8. Lorsque vous y êtes invité, appuyez sur la lettre <R> de votre clavier pour redémarrer IP-Reach.
 9. IP-Reach redémarre et l'écran d'initialisation d'IP-Reach s'affiche une fois le redémarrage effectué.



10. Félicitations ! IP-Reach est désormais prêt pour la connexion initiale.

Passez à la section suivante pour procéder à la première connexion à distance à IP-Reach. Une fois familiarisé avec le fonctionnement à distance d'IP-Reach, reportez-vous au **Chapitre 4 : Fonctions d'administration** pour connaître l'ensemble des fonctions d'administration proposées par IP-Reach.

Connexion à distance à IP-Reach

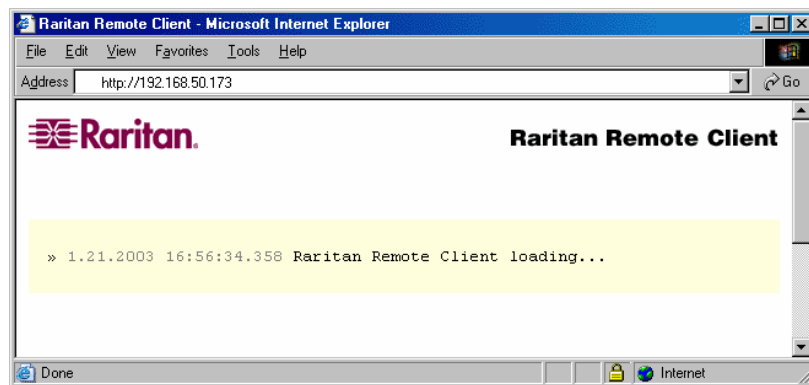
Une fois l'installation physique d'IP-Reach réalisée, vous pouvez établir votre première connexion réseau. Vous trouverez ci-dessous les instructions de base vous permettant de procéder à cette connexion. Pour obtenir des instructions détaillées, reportez-vous au **Chapitre 3 : Raritan Remote Client**.

Lancement de Raritan Remote Client (RRC)

1. Ouvrez une session sur un ordinateur Windows disposant d'un accès réseau à IP-Reach.
2. Si vous utilisez Windows NT, 2000 ou XP, vérifiez que vous ne disposez pas d'un accès restreint.
3. Lancez Microsoft Internet Explorer. Vérifiez que vos paramètres de sécurité Internet Explorer permettent le téléchargement et l'exécution des contrôles ActiveX.

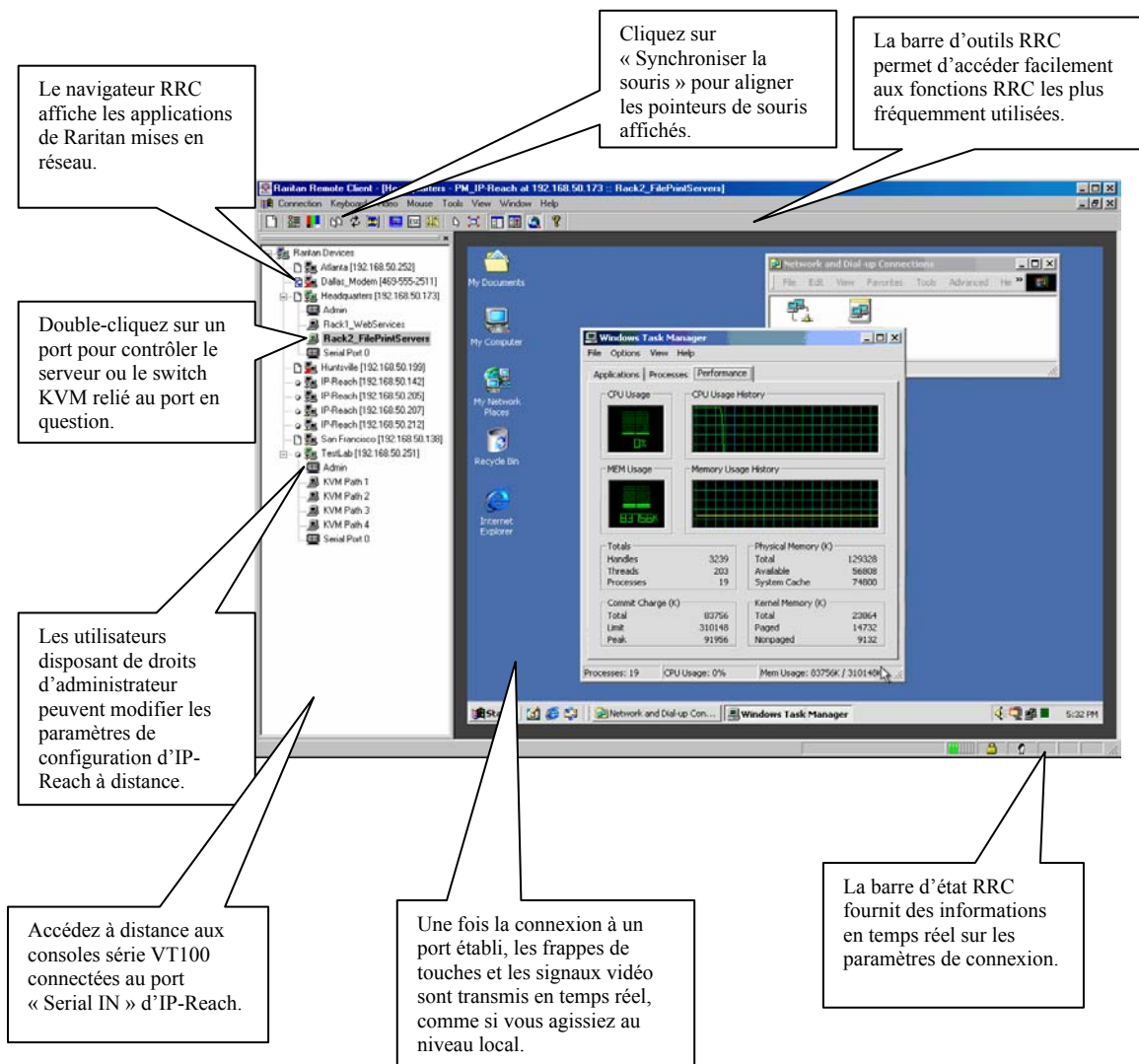
Remarque : le paramètre de sécurité « Moyen » par défaut de Windows est suffisant.

4. Dans la barre d'adresse URL, saisissez l'adresse IP affectée à IP-Reach à l'étape II-6. Appuyez sur [ENTREE] pour charger et lancer le client d'accès Web.



Définition d'une connexion

Lors du lancement de Raritan Remote Client (RRC), IP-Reach vous demande de saisir vos informations d'identification. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe par défaut (<admin> et <raritan>). Vous êtes désormais connecté à votre unité IP-Reach. Sélectionnez et connectez-vous à un port à l'aide du navigateur RRC, situé sur le côté gauche de la fenêtre RRC.



Remarque à l'intention des utilisateurs de CommandCenter

Si vous utilisez IP-Reach dans une configuration CommandCenter, suivez les étapes décrites ci-dessous lors de l'installation. Une fois les étapes de ce chapitre réalisées, veuillez vous reporter au guide d'utilisation de CommandCenter pour poursuivre l'installation. La suite de ce guide d'utilisation s'applique essentiellement aux utilisateurs qui déploient leur(s) unité(s) IP-Reach sans utiliser les fonctions d'intégration de CommandCenter.

Chapitre 3 : Raritan Remote Client

Activation de Raritan Remote Client (RRC) par l'intermédiaire d'un navigateur Web

Il est possible d'accéder à IP-Reach par l'intermédiaire d'un navigateur Web à l'aide d'une connexion établie depuis un ordinateur Windows distant exécutant Microsoft Internet Explorer 4.0+, Mozilla 1.1+ ou Netscape 7+.

Paramètres de sécurité

Si vous souhaitez accéder à IP-Reach par l'intermédiaire d'un navigateur Web, vous devez définir des paramètres adaptés au niveau de l'onglet des paramètres de sécurité Internet Explorer :

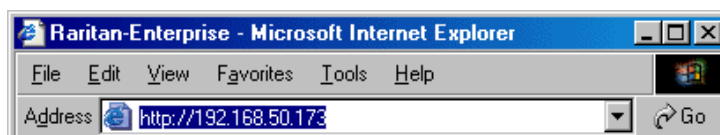
- l'option « Télécharger les contrôles ActiveX signés » doit être réglée sur « Activer » ou « Demander »,
- l'option « Exécuter les contrôles ActiveX et les plugins » doit être réglée sur « Activer » ou « Demander ».

Pour plus de détails sur ces paramètres, reportez-vous à votre documentation Microsoft Internet Explorer.

***Remarque :** quelles que soient les valeurs définies pour les paramètres ci-dessus dans Internet Explorer, Microsoft Windows 2000 et Microsoft Windows XP ne permettent pas à certains types d'utilisateurs de télécharger et d'exécuter les contrôles ActiveX et les plugins. Pour plus d'informations, reportez-vous à votre documentation Microsoft Windows.*

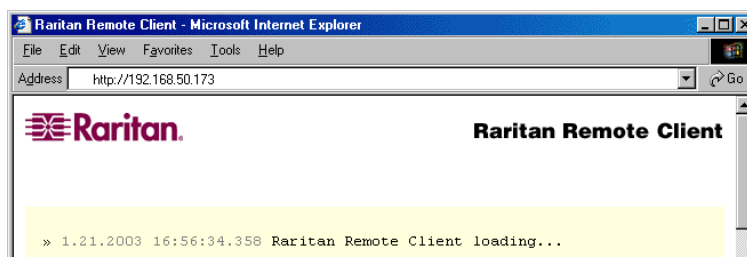
Lancement de Raritan Remote Client

1. Vérifiez que les paramètres de sécurité de votre navigateur sont configurés de manière adaptée et saisissez l'adresse IP affectée à votre unité IP-Reach (reportez-vous au **Chapitre 2 : Installation, Configuration initiale**) dans la barre d'adresse URL de votre navigateur Web.

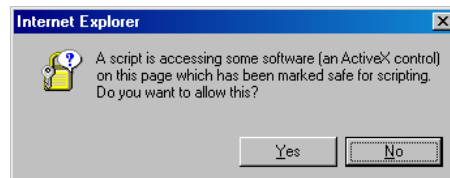
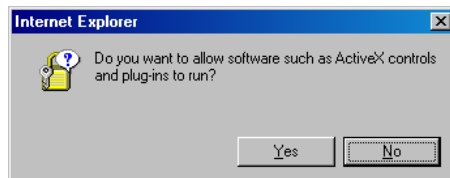
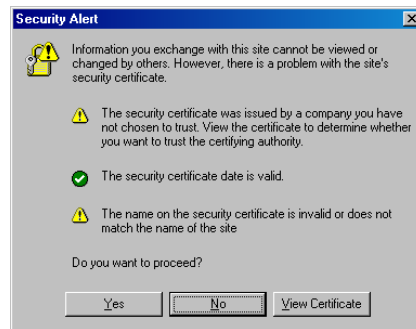


***Remarque :** IP-Reach est livré avec l'adresse IP par défaut suivante : 192.168.0.192.*

2. Pour le lancement de RRC, IP-Reach vous redirige vers un page Web sécurisée HTTPS (128 bits).



3. Selon les paramètres de sécurité définis pour votre navigateur, il est possible que toutes ou certaines des boîtes de dialogue suivantes s'affichent pour confirmer l'accès et le lancement d'un programme externe. Cliquez sur [Yes](Oui) pour passer à l'invite suivante.



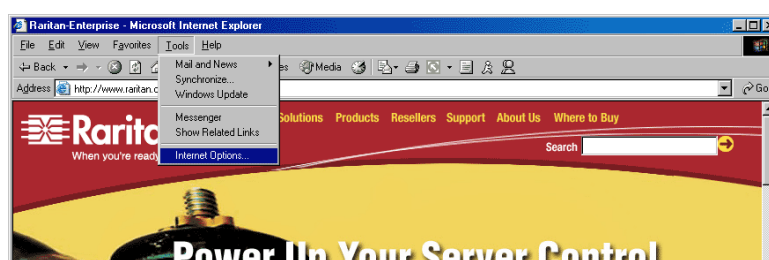
Remarque : quels que soient les paramètres définis dans Internet Explorer et que vous approuviez ou non les avertissements ci-dessus, Microsoft Windows 2000 et Microsoft Windows XP ne permettent pas à certains types d'utilisateurs de télécharger et d'exécuter les contrôles ActiveX et les plug-ins. Pour plus d'informations, veuillez vous reporter à la section précédente, « Paramètres de sécurité », et à votre documentation Microsoft Windows.

Suppression de RRC de la mémoire cache du navigateur

Si vous souhaitez supprimer RRC de la mémoire cache de votre navigateur pour procéder à une mise à niveau, pour économiser de l'espace disque ou pour supprimer les preuves de l'exécution de RRC sur un PC, par exemple, suivez la procédure standard indiquée par le logiciel de votre navigateur Web.

Instructions pour Internet Explorer version 6.0 :

1. Si vous avez utilisé RRC dernièrement, quittez et redémarrez Internet Explorer.
2. Dans la barre de menus Internet Explorer, sélectionnez **Outils** → **Options Internet**.



3. Lorsque la boîte de dialogue « Options Internet » s'affiche, cliquez sur « Paramètres ».
4. Lorsque la boîte de dialogue « Paramètres » s'affiche, cliquez sur « Afficher les objets ».
5. Internet Explorer affiche une liste des objets de programmes présents dans la mémoire cache. Sélectionnez et supprimez les entrées intitulées « TeleControl Class ».

Facultatif : installation du logiciel Raritan Remote Client

Remarque : cette étape est facultative. Vous pouvez accéder à IP-Reach à partir d'un ordinateur distant en installant le logiciel RRC ou en lançant RRC par l'intermédiaire d'un navigateur Web (reportez-vous à la section précédente). Si vous accédez à IP-Reach par l'intermédiaire d'un navigateur Web, il n'est pas nécessaire d'installer le logiciel sur l'ordinateur distant.

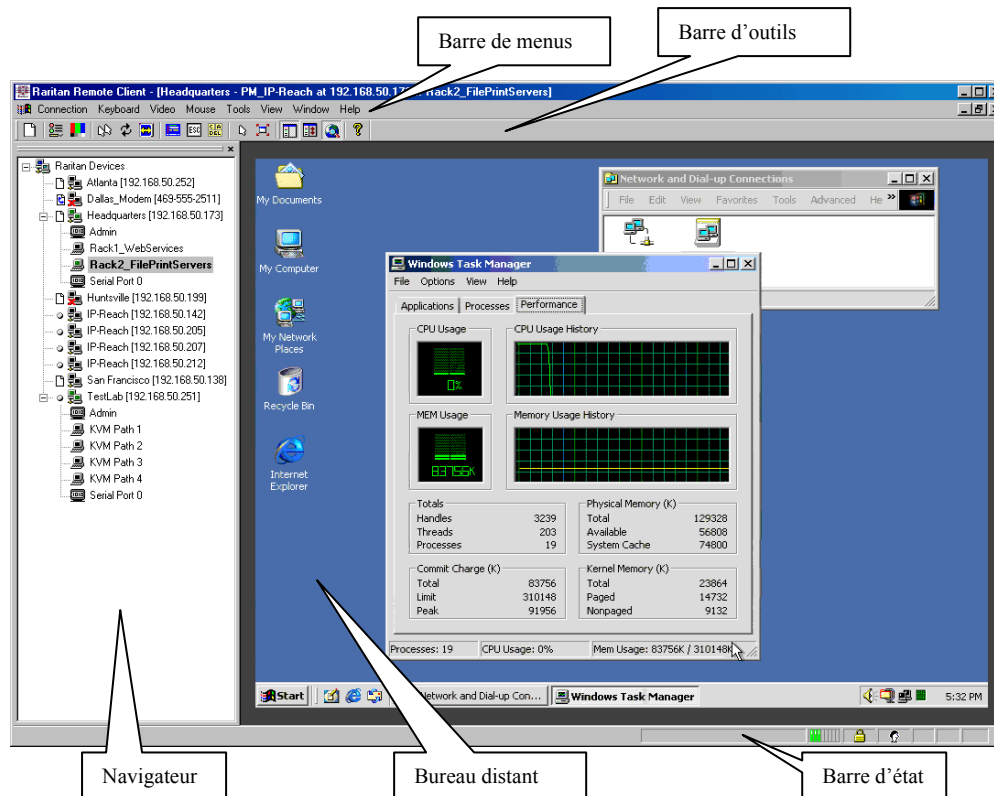
1. Insérez le CD-ROM RRC fourni dans le lecteur de CD-ROM de votre ordinateur.
2. Le programme d'installation de RRC se lance automatiquement. Si ce n'est pas le cas, cliquez avec le bouton droit de la souris sur le lecteur de CD-ROM de votre ordinateur dans l'Explorateur Windows et sélectionnez **Exécution automatique**.
3. Suivez les instructions affichées dans l'écran de l'assistant InstallShield pour procéder à l'installation de RRC sur votre ordinateur distant. Sous « Select Components » (Sélectionner les composants), vous devez sélectionner la version américaine si le clavier de l'ordinateur distant est un clavier américain ou la version japonaise si le clavier de l'ordinateur distant est un clavier japonais.

Remarque : la version japonaise de RRC permet d'utiliser un clavier japonais sur l'ordinateur distant mais nécessite également l'installation d'un clavier japonais au niveau du serveur cible. Les informations de l'interface sont toujours affichées en anglais.

4. Selon la configuration de votre ordinateur, il est possible que le programme d'installation de RRC installe automatiquement les bibliothèques Microsoft Foundation Class et DirectX, si nécessaire. Si tel est le cas, vous serez invité à redémarrer votre ordinateur une fois l'installation terminée.
5. Une icône Raritan Remote Client est ajoutée sur votre Bureau. Cliquez sur cette icône pour lancer RRC.

Disposition de la fenêtre RRC

Les fonctions de Raritan Remote Client sont réparties en cinq sections générales sur l'écran. Chaque section est décrite en détails plus loin dans ce chapitre.



Navigateur RRC

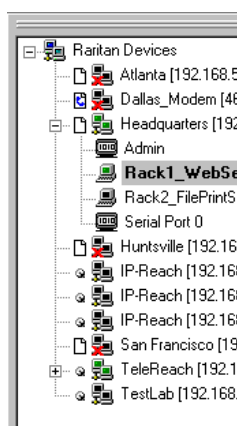
Le navigateur RRC offre une vue simple de l'ensemble des dispositifs Raritan connus. Vous pouvez ainsi accéder facilement à plusieurs applications Raritan mises en réseau.

Le navigateur RRC affiche :

- tous les dispositifs Raritan pour lesquels un *profil de connexion* existe,
- tous les dispositifs Raritan automatiquement identifiés sur le réseau.

Remarque : l'identification automatique des dispositifs Raritan fait appel à un protocole UDP et reconnaît généralement tous les dispositifs Raritan présents sur votre sous-réseau. Les administrateurs réseau autorisent rarement le fonctionnement du protocole UDP à l'extérieur du sous-réseau.

Remarque : l'identification automatique des dispositifs Raritan localise uniquement les dispositifs Raritan configurés de manière à utiliser le port TCP par défaut (5000).



Tous les dispositifs présents dans le navigateur RRC dispose de deux icônes permettant de connaître l'état du réseau et les informations relatives au profil de connexion.

Icône de gauche (profil de connexion)

	Avec profil - ce dispositif dispose d'un profil de connexion réseau.
	Profil modem - ce dispositif dispose d'un profil de connexion modem.
	Sans profil - RRC a localisé ce dispositif sur le réseau mais ce dispositif ne dispose d'aucun profil de connexion.

Icône de droite (état du réseau)

	Connecté (vert) - vous êtes actuellement authentifié et connecté à ce dispositif.
	Disponible (noir) - ce dispositif est actuellement disponible sur le réseau mais vous n'êtes pas connecté à ce dispositif pour l'instant.
	Non disponible - ce dispositif dispose d'un profil mais il n'est actuellement pas disponible sur le réseau (notez que tous les dispositifs disposant d'un profil modem auxquels vous n'êtes pas connecté pour l'instant affichent cette icône).

Le navigateur RRC étend l'arborescence d'affichage de tous les dispositifs Raritan auxquels vous êtes connecté afin d'afficher tous les ports auxquels vous avez accès.

- Les ports affichés avec une icône verte sont les ports auxquels vous êtes connecté.
- Les ports affichés en gras sont les ports actuellement affichés (actifs) dans la zone du Bureau distant du client.

Options du navigateur

Vous pouvez personnaliser certains attributs du navigateur RRC selon vos préférences.

	Afficher/Masquer le navigateur - affiche ou masque le navigateur RRC. Vous pouvez également activer cette option en sélectionnant View (Affichage) → Navigator (Navigateur) dans la barre de menus.
	Actualiser le navigateur - mise à jour des informations relatives à l'état des dispositifs affichés dans le navigateur RRC.
	Afficher les dispositifs détectés - indique si le navigateur RRC doit afficher les dispositifs localisés automatiquement sur le réseau pour lesquels aucun profil n'existe ou afficher uniquement les dispositifs qui disposent d'un profil. Vous pouvez également activer cette option en sélectionnant View (Affichage) → All Devices (Tous les dispositifs) dans la barre de menus.

Remarque : la méthode de connexion par exploration est la seule méthode permettant de se connecter à un dispositif Raritan configuré de manière à utiliser l'adressage IP DHCP.

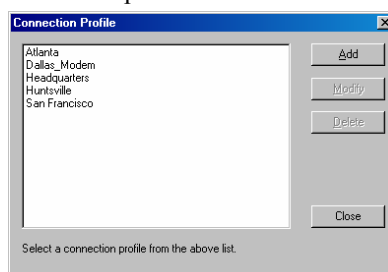
Création de nouveaux profils

Les profils de connexion permettent de stocker des informations importantes au sujet de votre dispositif Raritan telles que l'adresse IP, les ports TCP personnalisés, les paramètres de compression les plus couramment utilisés et les touches de sécurités personnalisées.

Remarque : si votre dispositif Raritan est configuré de manière à utiliser un port TCP personnalisé (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**) ou une touche de sécurité de groupe (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration de la sécurité**), vous devez d'abord créer un profil de connexion afin d'accéder au dispositif.

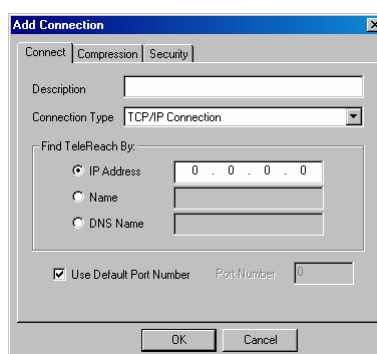
Pour créer un profil de connexion :

1. Sélectionnez **Connection (Connexion) → New Profile (Nouveau profil)** dans la barre de menus ou cliquez sur l'icône située la plus à gauche dans la barre d'outils. La boîte de dialogue Connection Profile (Profil de connexion), dans laquelle tous les profils de connexion existants sont répertoriés, s'affiche.



2. Cliquez sur [Add] (Ajouter).
3. La boîte de dialogue Add Connection (Ajouter une connexion) s'affiche. Les options sont regroupées sous trois onglets différents : **Connect (Connecter)**, **Compression** et **Security (Sécurité)**.

Onglet Connect (Connecter)



- **Description :** saisissez un nom permettant d'identifier facilement le dispositif Raritan que vous configurez actuellement, tel que « Centre de données_Atlanta », par exemple.

- **Connection Type (Type de connexion) :** sélectionnez l'option **TCP/IP Connection (Connexion TCP/IP)** si vous utilisez une connexion réseau local/réseau étendu ou l'option **Dial-Up Connection (Connexion d'accès à distance)** si vous utilisez une connexion modem analogique directe au dispositif Raritan.

Si vous utilisez une connexion TCP/IP, indiquez la méthode que RRC doit utiliser pour localiser votre dispositif Raritan :

- **IP Address (Adresse IP) :** adresse IP attribuée à votre dispositif Raritan (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**).
- **Name (Nom) :** nom attribué à votre dispositif Raritan lors de la configuration initiale (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**).

***Remarque :** si IP-Reach utilise l'adressage DHCP dynamique, sélectionnez l'option « Find IP-Reach by Name » (Trouver IP-Reach en fonction du nom).*

***Remarque :** le nom attribué par défaut à l'ensemble des unités IP-Reach est <IP-Reach>. Pour modifier le nom par défaut d'une unité IP-Reach et lui affecter un nom unique, reportez-vous au **Chapitre 4**.*

- **DNS Name (Nom DNS) :** si vous avez configuré votre serveur DNS de manière à affecter un nom DNS à l'adresse IP que vous avez attribuée à votre dispositif Raritan, utilisez ce nom DNS pour accéder à votre dispositif Raritan.

Si vous utilisez une Connexion d'accès à distance, saisissez les paramètres de connexion que RRC doit utiliser pour établir une connexion :

- **Phone Number (Numéro de téléphone) :** veillez à inclure les codes additionnels que RRC doit composer pour établir une connexion (indicatifs internationaux, indicatifs régionaux, codes d'accès des lignes extérieures, etc.).
- **Modem :** sélectionnez le modem, tel qu'il est configuré dans Windows, que RRC doit utiliser pour l'appel et la connexion à votre dispositif Raritan.

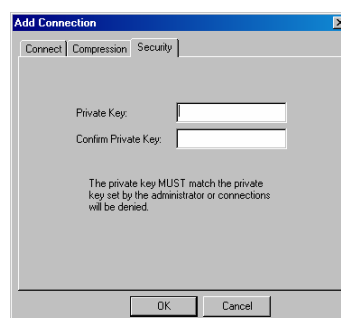
Sélectionnez le port TCP qui doit être utilisé :

- **Use Default Port Number (Utiliser le numéro de port par défaut) :** IP-Reach est configuré pour utiliser par défaut le port TCP 5000 lors de la communication avec RRC. Vous pouvez configurer IP-Reach de manière à ce qu'il utilise un port TCP différent (reportez-vous au **Chapitre 4 : Fonctions d'administration, Configuration réseau**). Si tel est le cas, désactivez la case d'option **Use Default Port Number (Utiliser le numéro de port par défaut)** et indiquez le port TCP configuré qui doit être utilisé.

Onglet Compression

Les paramètres de l'onglet Compression peuvent être définis par l'intermédiaire de RRC client. Ils ne sont donc pas nécessaires pour la configuration préalable dans la boîte de dialogue Connection Profile (Profil de connexion). Si vous souhaitez préconfigurer ces paramètres, reportez-vous à la section **Connexion et propriétés vidéo** de ce chapitre.

Onglet Security (Sécurité)



Si vous avez configuré votre unité IP-Reach de manière à ce qu'elle utilise une touche de groupe privée, saisissez cette touche ici afin d'être autorisé à établir une connexion avec cette unité IP-Reach. Une fois les champs remplis, cliquez sur [OK].

Une fois les écrans Connect (Connecter) et Security (Sécurité) remplis, cliquez sur [OK] pour terminer la création de la connexion.

Définition d'une nouvelle connexion

Pour vous connecter à un dispositif Raritan mis en réseau, il vous suffit de double-cliquer sur son entrée dans le navigateur RRC. Vous devez alors authentifier le dispositif.

***Remarque :** le nom d'utilisateur et le mot de passe par défaut de IP-Reach pour la connexion sont respectivement <admin> et <raritan>. Si vous vous connectez sous ce nom d'utilisateur et ce mot de passe, vous disposez des droits d'administrateur. Les mots de passe sont sensibles à la casse, ils doivent être saisis exactement de la même manière que lors de leur création. Le mot de passe par défaut <raritan> doit être saisi uniquement en lettres minuscules. Pour garantir la sécurité du système, modifiez le nom d'utilisateur et le mot de passe par défaut dès que possible.*

Si aucune entrée correspondant à votre unité IP-Reach ne figure dans le navigateur RRC, suivez les instructions de la section **Création de nouveaux profils** de ce chapitre pour créer un nouveau profil de connexion pour votre unité IP-Reach.

Si vous rencontrez des problèmes pour vous connecter à un dispositif Raritan, veuillez à vérifier les éléments suivants :

- **Nom d'utilisateur/Mot de passe :** les noms d'utilisateur et mots de passe de Raritan sont sensibles à la casse.
- **Port TCP :** si vous avez configuré votre dispositif Raritan de manière à ce qu'il utilise un port TCP autre que le port par défaut, vous devez saisir cette information dans le profil de connexion du dispositif.
- **Paramètres du pare-feu :** si vous accédez au dispositif Raritan par l'intermédiaire d'un pare-feu, ce dispositif doit être configuré de manière à autoriser la communication bidirectionnelle sur le port TCP 5000 (ou le port personnalisé pour lequel votre dispositif Raritan a été configuré).
- **Touche de sécurité :** si vous avez configuré votre dispositif Raritan de manière à ce qu'une touche de sécurité de groupe soit exigée, cette touche doit être saisie dans le profil de connexion du dispositif.

Fermeture d'une connexion à distance

Pour mettre fin à votre connexion à une unité IP-Reach, il vous suffit de cliquer avec le bouton droit de la souris sur l'entrée du dispositif dans le navigateur RRC et de sélectionner **Disconnect (Déconnecter)**.

Barre d'outils et raccourcis RRC



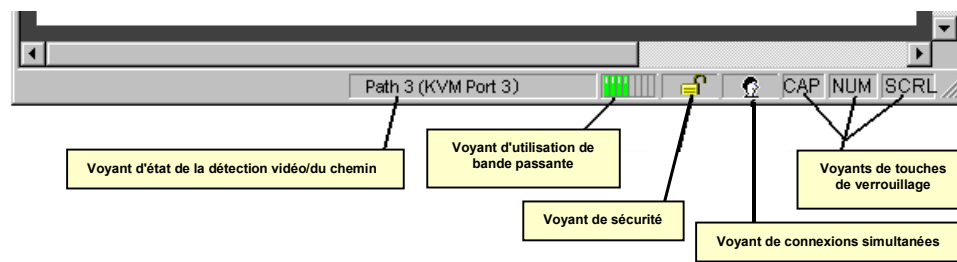
Barre d'outils Raritan Remote Client

La barre d'outils RRC permet d'accéder facilement et rapidement aux fonctions et paramètres de Raritan Remote Client les plus fréquemment utilisés :

BOUTON	NOM DU BOUTON	RACCOURCI-CLAVIER	FONCTION
	Nouveau profil	<Ctrl+Alt+C>	Nouveau profil <Ctrl+Alt+C> Permet de créer une nouvelle entrée dans le navigateur pour un dispositif Raritan (mêmes résultats que lors de la sélection de Connexion (Connexion) → New Profile (Nouveau profil) dans la barre de menus).
	Propriétés de la connexion	<Ctrl+Alt+P>	Permet d'ouvrir la boîte de dialogue Modify Connection Properties (Modifier les propriétés de la connexion) dans laquelle vous pouvez définir manuellement les options relatives à la bande passante (vitesse de connexion, profondeur de couleur, etc.).
	Paramètres vidéo	N/A	Permet d'ouvrir la boîte de dialogue Video Settings (Paramètres vidéo) dans laquelle vous pouvez définir manuellement les paramètres de conversion des signaux vidéo.
	Synchroniser la souris	<Ctrl+Alt+S>	En mode souris double, permet de forcer le réalignement du pointeur de la souris du serveur cible sur le pointeur de la souris du Raritan Remote Client.
	Actualiser l'écran	<Ctrl+Alt+R>	Permet de forcer l'actualisation de l'écran vidéo.
	Détection automatique des paramètres vidéo	<Ctrl+Alt+A>	Permet de forcer l'actualisation des paramètres vidéo (résolution, taux de rafraîchissement).
	Accéder au menu à l'écran	N/A	Permet d'accéder à l'interface utilisateur à l'écran du switch KVM connecté.
	Fermer le menu à l'écran	ECHAP	Permet de désactiver l'interface utilisateur à l'écran du switch KVM connecté.
	Envoyer Ctrl+Alt+Suppr	<Ctrl+Alt+D>	Permet d'envoyer une macro Ctrl+Alt+Suppr au serveur cible.
	Mode curseur simple	<Ctrl+Alt+X>	Permet d'accéder au mode curseur simple dans lequel le pointeur de la souris de l'ordinateur local ne s'affiche plus à l'écran. Pour quitter ce mode, appuyez sur <Ctrl+Alt+X>.
	Mode plein écran	<Ctrl+Alt+F>	Permet d'agrandir la zone de l'écran afin d'afficher le Bureau du serveur cible.
	Masquer/Afficher le navigateur	N/A	Permet d'afficher ou de masquer le navigateur RRC.
	Actualiser le navigateur	N/A	Permet de forcer l'actualisation des données affichées par le navigateur RRC.
	Afficher/Masquer les dispositifs détectés	N/A	Permet d'indiquer si le navigateur RRC doit afficher les dispositifs automatiquement identifiés sur le réseau (auquel aucun profil préconfiguré n'est associé).
	A propos de	N/A	Permet d'afficher les informations relatives à la version de Raritan Remote Client.

Barre d'état RRC

La **barre d'état** située au bas de la fenêtre Raritan Remote Client fournit des informations relatives à l'état de votre session de communication distante à IP-Reach.



Voyant d'état de la détection vidéo/du chemin

Indique si la détection vidéo est active.

Voyant d'utilisation de bande passante

Indique le pourcentage de bande passante actuellement utilisée. Le paramètre de vitesse de connexion, situé sous l'onglet Compression de l'écran Connection Properties (Propriétés de la connexion) indique la quantité de bande passante disponible.

Voyant de sécurité

Indique si la connexion à distance actuellement en cours est protégée par un cryptage. La configuration de cryptage requise est définie lors de la configuration d'IP-Reach (reportez-vous au **Chapitre 4**). Lorsqu'un dispositif IP-Reach est configuré avec l'option **No encryption (Pas de cryptage)** ou **SSL Authentication, NO data encryption (Authentification SSL, PAS de cryptage des données)**, l'indicateur de sécurité de la barre d'état est représenté sous la forme d'un cadenas ouvert. Lorsque l'option **SSL authentication, data encryption (Authentification SSL, cryptage des données)** ou **SSL authentication, SSL encryption (Authentification SSL, cryptage SSL)** est sélectionnée, l'indicateur de sécurité de la barre d'état est représenté sous la forme d'un cadenas fermé.

Voyant de connexions simultanées

Indique si plusieurs utilisateurs distants sont actuellement connectés à la même unité IP-Reach (si un seul utilisateur est connecté, une icône s'affiche, si deux utilisateurs ou plus sont connectés, deux icônes s'affichent).

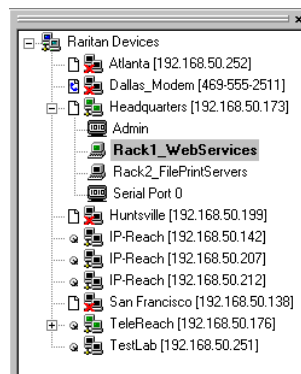
Les options de connexions simultanées peuvent être définies globalement sous **PC Share Mode (Mode PC-Share)** dans l'écran Security Configuration (Configuration de la sécurité) (reportez-vous au **Chapitre 4**) ou pour chaque utilisateur à l'aide du paramètre **Concurrent Access Mode (Mode d'accès simultané)** dans l'écran User Account Settings (Paramètres des comptes utilisateur) (reportez-vous au **Chapitre 4**).

Voyants de touches de verrouillage

Indiquent l'état du serveur cible au regard de l'activation des touches de verrouillage des majuscules, de verrouillage numérique et de l'arrêt du défilement. Si ces touches sont activées sur le serveur cible affiché, cet état s'affiche sur la barre d'état comme indiqué.

Contrôle de la console KVM distante

Une fois le navigateur RRC utilisé pour établir une connexion avec une unité IP-Reach (reportez-vous à la section précédente : **Définition d'une nouvelle connexion**), l'entrée correspondant à l'unité IP-Reach dans le navigateur se développe de manière à afficher tous les ports d'IP-Reach permettant un accès à distance.

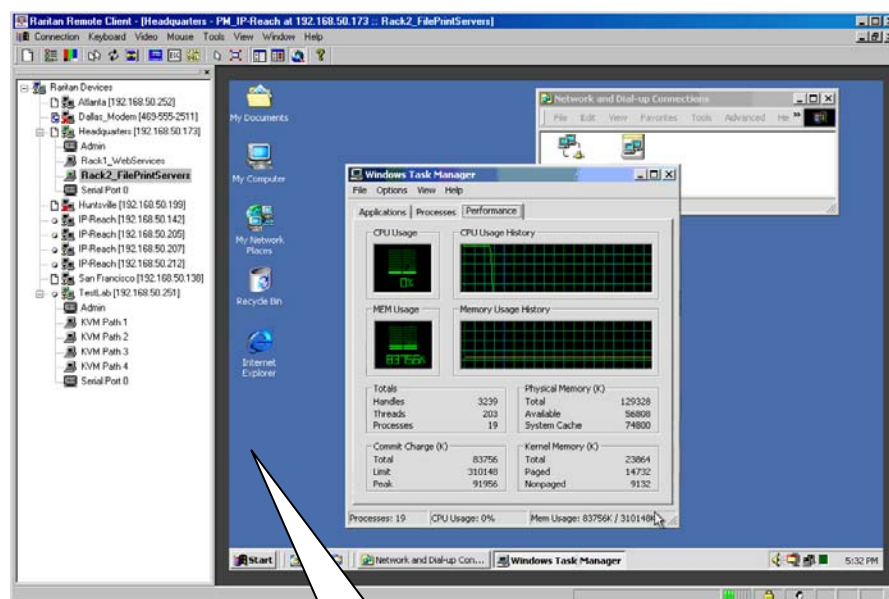


Pour établir une connexion avec la console KVM distante, il vous suffit de double-cliquer sur le port KVM que vous souhaitez contrôler.

Une fois connecté, IP-Reach affiche la sortie vidéo en temps réel du switch KVM ou du serveur connecté au port KVM d'IP-Reach. Ce signal vidéo est compressé et crypté selon les paramètres de configuration définis par l'administrateur (reportez-vous au **Chapitre 4**).

Une fois connecté à un switch KVM ou à un serveur, vous disposez d'un contrôle à faible niveau complet sur la console KVM, comme si vous vous trouviez physiquement à côté du switch KVM ou du serveur.

Lorsque le pointeur de votre souris se trouve dans la zone du Bureau distant de RRC, les mouvements et les clics de souris sont directement transmis au switch KVM ou au serveur distant connecté.



Zone du Bureau distant

Mode souris simple/Mode souris double

Lorsque vous affichez à distance un serveur cible qui utilise un dispositif de pointage, deux pointeurs de souris s'affichent par défaut dans le Bureau distant de la fenêtre Raritan Remote Client. Le pointeur de la souris de Raritan Remote Client, généré par le système d'exploitation sur lequel RRC est exécuté, dirige légèrement le pointeur de la souris du serveur cible lors des mouvements. Cette opération est le résultat nécessaire du retard numérique.

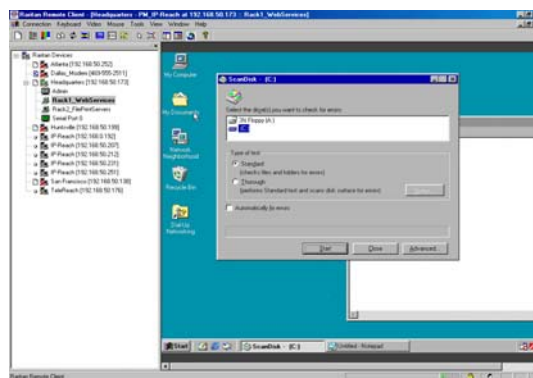
Avec les connexions réseau local rapides, il arrive cependant que certains utilisateurs préfèrent désactiver le pointeur de la souris de Raritan Remote Client et afficher uniquement le pointeur de la souris du serveur cible lors des opérations. Pour passer d'un mode à l'autre, utilisez le raccourci-clavier **<Ctrl+Alt+X>** ou cliquez sur l'icône de mode **Single Mouse Pointer (Pointeur de souris simple)** dans la barre d'outils RRC.

Remarque : pour obtenir un meilleur alignement des deux pointeurs de souris en mode souris double, cliquez sur le bouton **[Synchroniser la souris]** de la barre d'outils RRC ou appuyez simultanément sur les touches **<Ctrl+Alt+S>**. Cette opération permet de forcer le réalignement des deux pointeurs de souris. Si, après avoir suivi soigneusement les instructions de la section « Configuration des serveurs cible » du chapitre 2, vous ne parvenez toujours pas à synchroniser les pointeurs de souris, cliquez sur le bouton **[Détection automatique des signaux vidéo]** de la barre d'outils RRC.

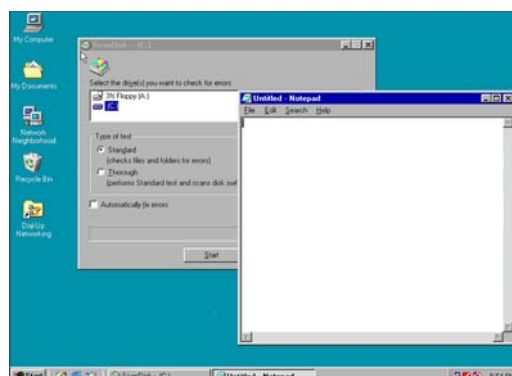
Mode plein écran

Le mode plein écran de Raritan Remote Client permet d'agrandir la zone d'écran RRC disponible de manière à afficher le Bureau distant en supprimant les bordures des fenêtres, les barres d'état et le navigateur RRC.

Cette option est particulièrement utile lors de l'affichage d'un serveur cible dont la résolution vidéo est égale ou supérieure au paramètre de résolution vidéo de l'ordinateur sur lequel RRC est exécuté, lors de l'affichage d'un serveur 1024 x 768 sur un ordinateur 1024 x 768, par exemple.



Affichage standard



Affichage en mode plein écran

Pour passer en mode plein écran, cliquez sur l'icône Mode plein écran de la barre d'outils RRC (ou appuyez sur les touches de raccourci-clavier **<Ctrl+Alt+F>**). Pour quitter le mode plein écran, appuyez sur les touches de raccourci-clavier **<Ctrl+Alt+F>**.

Sélection de serveurs avec un switch KVM

Deux boutons permettent aux utilisateurs d'accéder rapidement à l'interface utilisateur à l'écran mise à disposition par votre switch KVM. Les boutons **[Activer l'interface utilisateur à l'écran]** et **[Quitter l'interface utilisateur à l'écran]** de la barre d'outils RRC sont conçus pour simplifier l'utilisation d'IP-Reach en association avec des switch KVM.

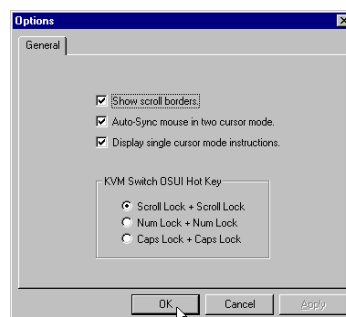
	Activer l'interface utilisateur à l'écran
	Quitter l'interface utilisateur à l'écran

Les étapes ci-dessous permettent de configurer RRC de manière à activer et quitter les interfaces utilisateur des switch KVM utilisés en association avec RRC. Une fois IP-Reach configuré conformément au raccourci-clavier de votre switch KVM, vous pouvez sélectionner les serveurs cible à l'aide des deux boutons de la barre d'outils RRC mentionnés ci-dessus.

Remarque : pour accéder à l'interface utilisateur à l'écran KVM, les utilisateurs distants peuvent également saisir le raccourci-clavier du switch KVM sur le clavier de l'ordinateur distant. Ce principe s'applique aussi bien aux produits KVM Raritan qu'aux produits KVM d'autres marques.

Si vous souhaitez utiliser les icônes de commutation de RRC, IP-Reach doit être configuré de manière à déclencher le raccourci-clavier de l'interface utilisateur à l'écran du switch KVM connecté. Il s'agit d'une procédure d'installation unique qu'il n'est pas utile de répéter par la suite, à moins que la désignation du raccourci-clavier du switch KVM soit modifiée.

1. Vous pouvez utiliser la touche **<Arrêt défil>**, **<Verr num>** ou **<Verr. maj.>** en guise de raccourci-clavier de l'interface utilisateur à l'écran. Localisez le raccourci-clavier qui permet d'activer l'interface utilisateur à l'écran de votre switch KVM. S'il n'existe aucun raccourci-clavier de ce type, vous pouvez créer une macro de clavier (reportez-vous à la section suivante) afin qu'elle accomplisse la même tâche.
2. Dans la barre de menus RRC, sélectionnez **Tools (Outils) → Options**.



3. Sélectionnez le raccourci-clavier qui permet d'activer l'interface utilisateur à l'écran du switch KVM connecté.
4. Cliquez sur **[OK]** pour poursuivre.

Macros de clavier

RRC permet aux utilisateurs de créer des macros de clavier personnalisées permettant d'envoyer des séquences de touches données au serveur distant ou au switch KVM connecté à IP-Reach. Cette fonction permet aux clients d'envoyer des frappes de touches aux serveurs distants. Sans elle, les frappes risqueraient d'être interprétées involontairement par l'ordinateur sur lequel RRC est exécuté.

La fonction de macros de clavier d'IP-Reach permet de garantir que les combinaisons de touches destinées au serveur cible sont bien envoyées et qu'elles sont interprétées par le serveur cible uniquement.

Macro Ctrl+Alt+Suppr

Une macro Ctrl+Alt+Suppr a été, en raison de son utilisation fréquente, programmée au préalable dans Raritan Remote Client. Elle permet d'illustrer les possibilités des macros de clavier.

	Envoyer Ctrl+Alt+Suppr	<Ctrl+Alt+D>	Permet d'envoyer une macro Ctrl+Alt+Suppr au serveur cible.
---	---------------------------	--------------	---

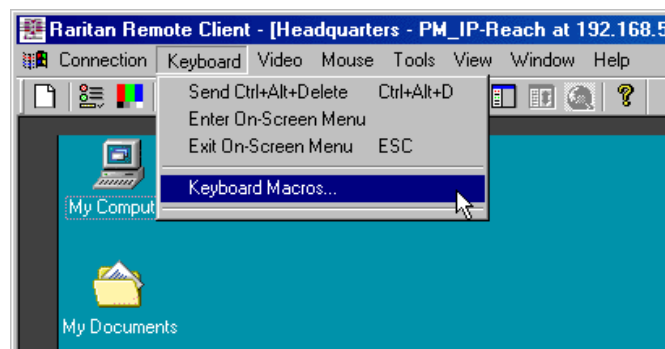
Lorsque vous cliquez sur l'icône Ctrl+Alt+Suppr de la barre d'outils RRC, cette séquence de touches est envoyée au serveur ou au switch KVM auquel vous êtes actuellement connecté. Par opposition, si vous appuyiez sur les touches Ctrl+Alt+Suppr de votre clavier lors de l'utilisation de RRC, la commande serait d'abord interceptée par votre propre ordinateur en raison de la structure du système d'exploitation Windows, au lieu d'être envoyée au serveur cible comme prévu.

Définition d'une macro de clavier

Les instructions suivantes détaillent les étapes nécessaires à la création d'une macro de clavier pour la commande Windows « Minimiser toutes les fenêtres/Bureau ».

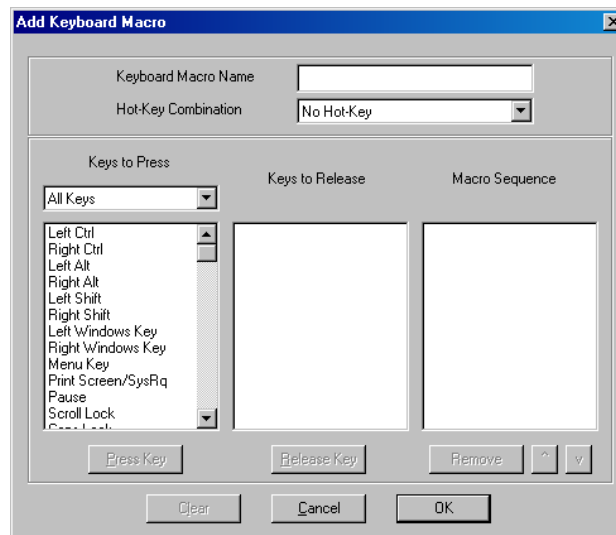
sous Windows, si vous appuyez sur les touches <**Windows+D**>, toutes les fenêtres du programme sont réduites. Cependant, lorsque vous êtes connecté au serveur cible à l'aide de RRC, la macro de clavier est le seul moyen d'effectuer cette tâche sur le serveur cible car, une fois encore, si vous appuyez sur les touches <**Windows+D**> de votre clavier, votre propre ordinateur client intercepte et exécute la commande au lieu de l'envoyer au serveur cible comme prévu.

1. Dans la barre de menus RRC, sélectionnez **Keyboard (Clavier) → Keyboard Macros (Macros de clavier)**.

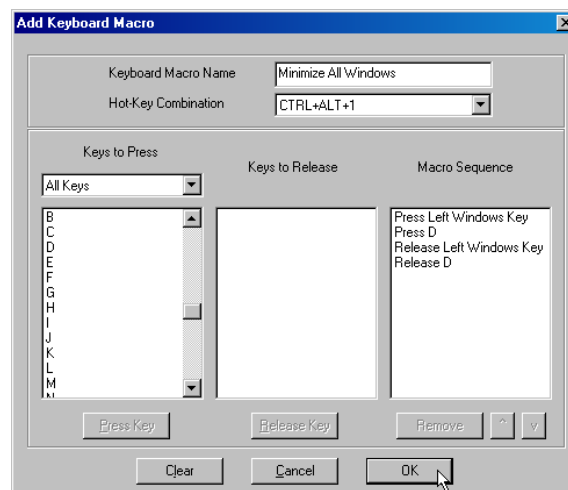


2. Lorsque la boîte de dialogue Keyboard Macros (Macros de clavier) s'ouvre, cliquez sur [Add] (Ajouter).

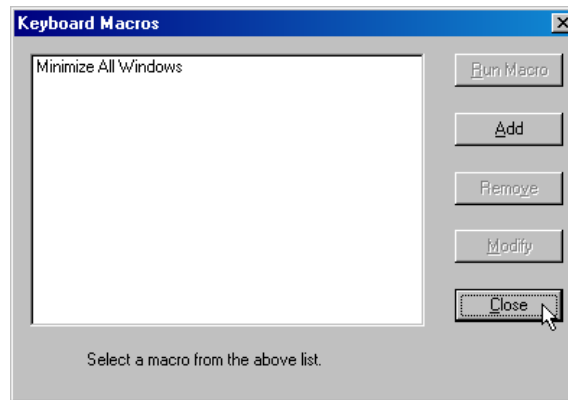
3. La boîte de dialogue Add Keyboard Macro (Ajouter une macro de clavier) s'ouvre.



4. Définissez la macro de clavier en renseignant les champs de la fenêtre Add Keyboard Macro (Ajouter une macro de clavier) dans l'ordre indiqué ci-dessous. Cliquez sur [OK] lorsque vous avez terminé.
- Saisissez un nom dans le champ **Keyboard Macro Name (Nom de la macro de clavier)**. Une fois la macro de clavier créée, le nom saisi s'affichera dans la barre de menus RRC. Dans le cadre de notre exemple, « Minimiser toutes les fenêtres ».
 - Facultatif** : dans le champ **Hot-Key Combination (Raccourci-clavier)**, indiquez une association de touches qui permettra de lancer facilement la macro à partir du clavier lors de l'exécution de RRC. Dans le cadre de notre exemple « Minimiser toutes les fenêtres », nous avons sélectionné **<Ctrl+Alt+I>**.
 - Dans la zone de sélection **Keys to Press (Touches à enfoncer)**, sélectionnez les touches pour lesquelles vous souhaitez émuler des frappes de touches, dans l'ordre dans lequel les touches seront enfoncées. Cliquez sur [Press Key] (Appuyer sur la touche) après chaque sélection. Une fois les touches sélectionnées, elles apparaissent dans la zone de sélection **Keys to Release (Touches à relâcher)**, située au centre de la boîte de dialogue.
 - Dans le cadre de notre exemple « Minimiser toutes les fenêtres », nous demandons la transmission de deux touches : la touche **<Windows>** et la touche de la lettre **<D>**.
 - Dans la zone de sélection **Keys to Release (Touches à relâcher)**, sélectionnez les touches pour lesquelles vous souhaitez émuler des frappes de touches, dans l'ordre dans lequel les touches seront relâchées. Cliquez sur [Release Key] (Relâcher la touche) après chaque sélection.
 - Dans le cadre de notre exemple « Minimiser toutes les fenêtres », nous demandons à ce que les deux touches enfoncées soient également relâchées.
 - Vérifiez la zone de texte **Macro Sequence (Séquence de la macro)**, dont le contenu est généré automatiquement, afin de vous assurer que le déroulement de la macro est le reflet exact de la séquence de touches souhaitée. Si nécessaire, ajustez le contenu et l'ordre de votre macro à l'aide du bouton [Remove] (Supprimer) et des boutons en forme de flèches.



5. Cliquez sur [OK]. La boîte de dialogue Keyboard Macros (Macros de clavier), dans laquelle votre nouvelle macro de clavier est répertoriée, s'affiche alors.



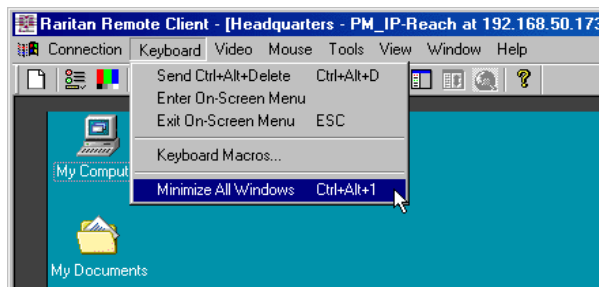
6. Cliquez sur [Close] (Fermer) pour finir la procédure d'édition de la macro de clavier.

Lancement d'une macro de clavier

Une fois la macro créée, elle peut être exécutée par l'intermédiaire de la barre de menus RRC ou du raccourci-clavier défini lors de la création de la macro (le cas échéant).

Activation de la barre de menus

Une fois la macro créée, elle apparaît dans le menu Keyboard (Clavier) de la barre de menus RRC. Il vous suffit de cliquer sur l'entrée de votre nouvelle macro de clavier pour exécuter cette dernière.



Activation du raccourci-clavier

Une fois la macro créée, elle peut également être exécutée, lors de l'utilisation de RRC, à l'aide du raccourci-clavier affecté (le cas échéant) à la macro. Dans le cadre de l'exemple « Minimiser toutes les fenêtres » détaillé ci-dessus, l'utilisateur peut, lors de l'utilisation de RRC, appuyer simultanément sur les touches <Ctrl+Alt+1> pour envoyer l'association de touches <Windows+D> au serveur cible.

Connexion et propriétés vidéo

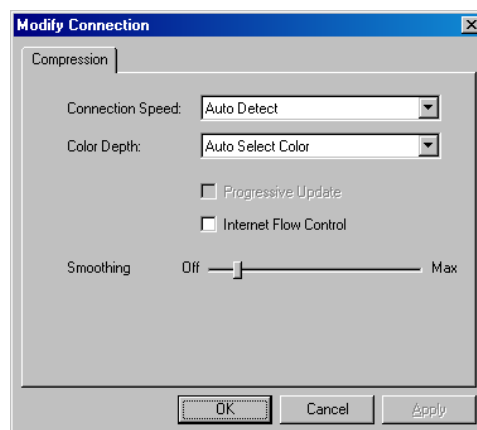
Les algorithmes de compression vidéo dynamique d'IP-Reach maintiennent le caractère convivial des consoles KVM avec différents types de bande passante. A la différence des solutions concurrentes, IP-Reach optimise sa sortie KVM non seulement pour l'utilisation en réseau local mais également par l'intermédiaire du réseau étendu et de l'accès à distance. En ajustant de manière dynamique la profondeur de couleur et en limitant la sortie vidéo, IP-Reach offre l'équilibre idéal entre qualité vidéo et temps de réponse du système pour n'importe quel type de bande passante.

Les utilisateurs de RRC doivent comprendre les paramètres réglables suivants des boîtes de dialogue **Connection Properties (Propriétés de la connexion)** et **Video Settings (Paramètres vidéo)** et se familiariser avec leurs effets respectifs. Ils peuvent être optimisés selon vos besoins sous différents systèmes d'exploitation.

Propriétés de la connexion

	Propriétés de la connexion	<Ctrl+Alt+P>	Permet d'ouvrir la boîte de dialogue Modify Connection Properties (Modifier les propriétés de la connexion) dans laquelle vous pouvez définir manuellement les options relatives à la bande passante (vitesse de connexion, profondeur de couleur, etc.).
---	----------------------------	--------------	---

Pour accéder à la boîte de dialogue Connection Properties (Propriétés de la connexion), sélectionnez **Connection (Connexion)** → **Connection Properties (Propriétés de la connexion)** dans la barre de menus RRC ou cliquez sur [**Propriétés de la connexion**] dans la barre d'outils RRC.



Connection Speed (Vitesse de connexion)

La zone de sélection Connection Speed (Vitesse de connexion) permet aux utilisateurs de limiter manuellement l'utilisation de la bande passante réseau par IP-Reach selon une quantité définie. IP-Reach détecte normalement automatiquement la quantité de bande passante disponible. Le paramètre Connection Speed (Vitesse de connexion) permet aux utilisateurs d'informer manuellement IP-Reach d'une limitation de la bande passante : IP-Reach adapte alors son comportement et se contente d'utiliser la quantité de bande passante disponible.

Color Depth (Profondeur de couleur)

Pour la plupart des tâches d'administration (surveillance de serveur, reconfiguration, etc.), les administrateurs de serveurs ne nécessitent pas l'ensemble du spectre de couleurs 24 bits ou 32 bits, disponible avec la plupart des cartes graphiques modernes. Si vous tentez de transmettre des images avec des profondeurs de couleur si élevées, vous risquez en effet de perdre une quantité importante de la précieuse bande passante réseau.

IP-Reach peut adapter de manière dynamique la profondeur de couleur transmise aux utilisateurs distants afin d'optimiser le caractère convivial pour n'importe quel type de bande passante.

- Option **Progressive Update (Mise à jour progressive)** : La fonction Progressive Update (Mise à jour progressive) extrêmement novatrice d'IP-Reach permet d'accroître le niveau de convivialité dans les environnements dont la quantité de bande passante est limitée. Lorsque l'option Progressive Update (Mise à jour progressive) est activée, IP-Reach envoie d'abord une image à faible profondeur de couleur au Bureau distant. Il fournit ensuite des images avec une profondeur de couleur plus élevée, autorisée par la bande passante.

La philosophie de cette option est très similaire à la notion World Wide Web courante de fichiers « GIF entrelacés ».

Remarque : lorsque le paramètre *Color Depth (Profondeur de couleur)* est défini sur **Auto Select Color (Sélection automatique des couleurs)** (valeur par défaut), l'option **Progressive Update (Mise à jour progressive)** est activée. IP-Reach active ou désactive l'option *Progressive Update (Mise à jour progressive)* selon la vitesse de connexion (il active l'option pour les connexions rapides et la désactive pour les connexions lentes).

Internet Flow Control (Contrôle du flux Internet)

De nombreux réseaux étendus publics sont, de par leur nature même, instables. Les paquets envoyés sur l'Internet public ne parviennent pas nécessairement à destination dans l'ordre dans lequel ils ont été expédiés. Lors de l'utilisation d'IP-Reach sur un réseau étendu public instable (notamment dans les scénarios internationaux), l'activation de l'option Internet Flow Control (Contrôle du flux Internet) permet de garantir que les paquets transmis par IP-Reach sont reçus et réassemblés par RRC dans le bon ordre.

Smoothing (Lissage)

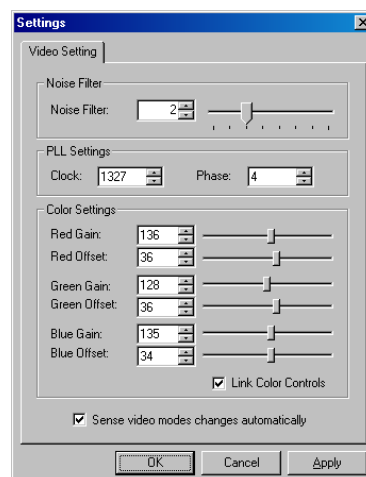
Le niveau de lissage vidéo indique à IP-Reach le degré d'importance des changements de dégradés de couleurs pour la transmission. Des valeurs de couleur approximatives sont affectées aux pixels vidéo qui vagabondent à partir de la couleur majoritaire afin de réduire l'utilisation de bande passante et la transmission de bruit vidéo. Si les niveaux de lissage définis sont trop élevés, des inexactitudes peuvent se produire au niveau des couleurs. Le fait de définir des niveaux de lissage moins importants nécessite une bande passante plus large et une puissance de traitement plus élevée.

Paramètres vidéo

	Paramètres vidéo	N/A	Permet d'ouvrir la boîte de dialogue Video Settings (Paramètres vidéo) dans laquelle vous pouvez définir manuellement les paramètres de conversion des signaux vidéo.
---	------------------	-----	---

Pour accéder à la boîte de dialogue Video Settings (Paramètres vidéo), sélectionnez **Video (Vidéo) → Video Settings (Paramètres vidéo)** dans la barre de menus RRC ou cliquez sur le bouton **Connection Properties (Propriétés de la connexion)** dans la barre d'outils RRC.

Il est possible d'actualiser la plupart des paramètres de cette boîte de dialogue en procédant à un calibrage des couleurs, comme indiqué à la section suivante, ou en forçant manuellement IP-Reach à détecter automatiquement les paramètres vidéo (dans la barre de menus RRC, sélectionnez **Video (Vidéo) → Auto-sense Video Settings (Détection automatique des paramètres vidéo)**). Il est néanmoins utile que les utilisateurs connaissent la signification et les implications des différents paramètres.



Noise Filter (Filtre antiparasite)

La sortie vidéo des cartes graphiques, transmise sous forme analogique, peut être soumise à des bruits provoqués par des interférences et à des bruits électriques. Le système avancé d'IP-Reach peut filtrer ces faibles variations, erronées et involontaires, des signaux de manière à optimiser la qualité des images et la quantité de bande passante utilisée.

Plus élevée : les paramètres Noise Filter (Filtre antiparasite) demandent à IP-Reach de transmettre un pixel vidéo de variante uniquement s'il existe une importante variation de couleurs par rapport à ses voisins.

Néanmoins, si vous définissez un seuil trop élevé, des modifications souhaitées au niveau de l'écran peuvent être filtrées de manière non intentionnelle.

Plus faible : les paramètres Noise Filter (Filtre antiparasite) demandent à IP-Reach de transmettre la plupart des modifications au niveau des pixels. Si le seuil défini est trop faible, l'utilisation de la bande passante risque d'être plus importante.

Remarque : les paramètres Noise Filter (Filtre antiparasite) plus faibles (de 1 à 4 environ) sont recommandés. Les paramètres plus élevés mettent fin à la transmission superflue de mauvaises variations de couleurs. Cependant, les petites modifications réelles et intentionnelles au niveau de l'image vidéo risque de ne pas être transmises.

Paramètres analogique/numérique

Nous vous recommandons de laisser IP-Reach détecter automatiquement les paramètres suivants (dans la barre de menus RRC, sélectionnez **Video (Vidéo)** → **Auto-sense Video Settings (Détection automatique des paramètres vidéo)**). Une description relative à chacun des paramètres est néanmoins proposée ici.

- **PLL Settings (Paramètres PPL)** : si l'image vidéo semble très floue ou que sa mise au point ne semble pas correcte, les paramètres PPL pour l'horloge et la phase peuvent être ajustés jusqu'à ce qu'une image de meilleure qualité s'affiche sur le serveur cible actif.
 - **Clock (Horloge)** : diviseur de synchronisation horizontale permettant de produire l'horloge de pixels. Contrôle la vitesse d'affichage des pixels vidéo sur l'écran vidéo. Les modifications apportées aux paramètres de l'horloge entraînent l'étirement ou la réduction de l'image vidéo sur le plan horizontal. Nous vous recommandons d'indiquer des nombres impairs.
 - **Phase** : les valeurs de phase sont comprises entre 0 et 31 et s'affichent en boucle. Arrêtez le réglage sur la valeur de phase qui permet d'obtenir l'image vidéo de meilleure qualité pour le serveur cible actif.
- **Color Settings (Paramètres Couleur)** : il est possible de définir le contrôle de gain comme un réglage du contraste. Il est possible de définir le contrôle du décalage comme un réglage de la luminosité.
 - **Red Gain (Gain du rouge)** : contrôle l'amplification du signal rouge.
 - **Red Offset (Décalage du rouge)** : contrôle l'inclinaison du signal rouge.
 - **Green Gain (Gain du vert)** : contrôle l'amplification du signal vert.
 - **Green Offset (Décalage du vert)** : contrôle l'inclinaison du signal vert.
 - **Blue Gain (Gain du bleu)** : contrôle l'amplification du signal bleu.
 - **Blue Offset (Décalage du bleu)** : contrôle l'inclinaison du signal bleu.
 - **Link Color Controls (Lier les contrôles des couleurs)** : permet de déplacer l'ensemble des barres de défilement du gain lorsque la barre de défilement du gain d'une couleur est déplacée et de déplacer l'ensemble des barres de défilement du décalage lorsque la barre de défilement du décalage d'une couleur est déplacée.
- **Sense video mode changes automatically (Détecter automatiquement les modifications du mode vidéo)** : indique si IP-Reach doit actualiser automatiquement l'image vidéo envoyée à RRC lorsqu'il détecte une modification au niveau de la résolution vidéo ou des taux de rafraîchissement du serveur cible.

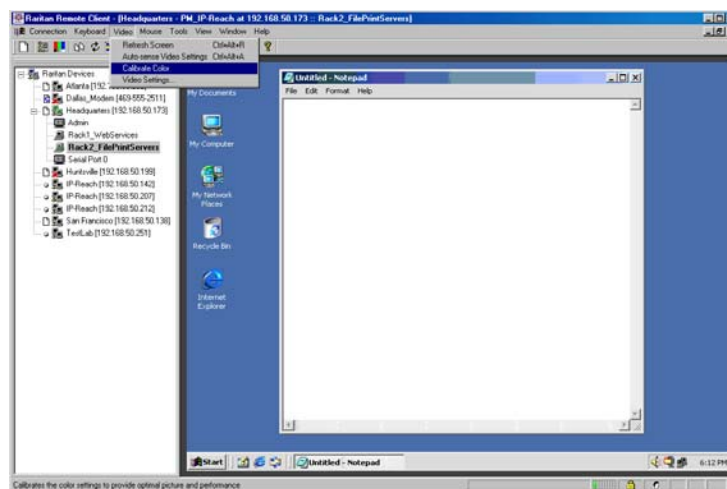
Calibrage des couleurs

Le calibrage automatique des couleurs ajuste les paramètres de couleur d'IP-Reach afin de réduire le bruit de couleur superflu et les données lors de la numérisation des images vidéo. Cette optimisation des données permet d'augmenter les performances opérationnelles d'IP-Reach et notamment la précision des couleurs.

Utilisez le calibrage des couleurs, une procédure très simple à réaliser, lorsque les niveaux de couleur (teinte, luminosité, saturation) des images vidéo transmises ne semblent pas corrects. Les paramètres de couleur d'IP-Reach ne subissent aucune modification lorsque vous passez d'un ordinateur cible à un autre. Le fait de procéder au calibrage des couleurs sur un serveur cible représentatif affecte donc l'ensemble des serveurs cible connectés.

Pour procéder au calibrage des couleurs :

1. Etablissez une connexion KVM distante avec les serveurs exécutant une interface utilisateur graphique.
2. Assurez-vous que la couleur blanche solide recouvre environ 15 % ou plus du Bureau du serveur cible. Il vous suffit pour cela d'ouvrir l'application Notepad et d'agrandir sa fenêtre à la taille de l'écran.



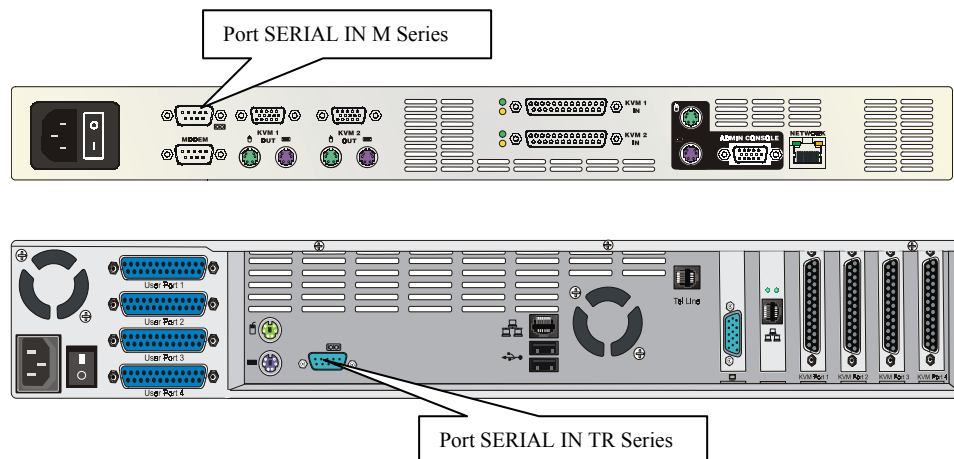
3. Dans la barre de menus RRC, sélectionnez **Video (Vidéo) → Calibrate Color (Calibrer les couleurs)** pour procéder au calibrage des couleurs.

Contrôle série à distance

Avec IP-Reach, les utilisateurs peuvent accéder aux consoles KVM distantes mais également aux consoles série à l'aide d'un navigateur Web. Les consoles série prenant en charge l'émulation VT100 peuvent être connectées au port d'ENTREE SERIE, situé sur le panneau arrière d'IP-Reach. L'accès est réalisé à l'aide de Raritan Remote Client.

Connexion physique

Le port d'ENTREE SERIE situé sur le panneau arrière d'IP-Reach est un connecteur mâle DB9 équipé d'une broche DTE RS-232 standard.

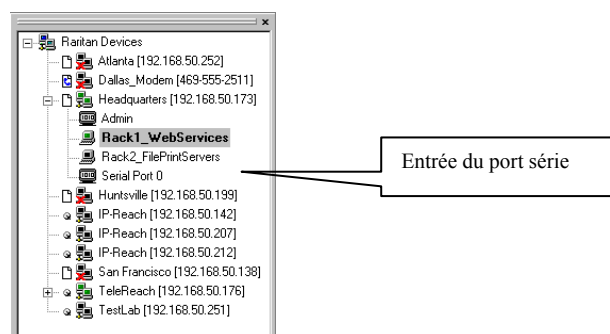


Lors de la connexion de votre dispositif série au port d'ENTREE SERIE d'IP-Reach, veuillez à utiliser :

- un câble série à brochage direct permettant la connexion des consoles DCE,
- un câble série null-modem permettant la connexion des consoles DTE.

Connexion à distance

Pour établir une connexion à distance avec la console série connectée au port d'ENTREE SERIE de votre unité IP-Reach, double-cliquez sur l'entrée du dispositif série dans le navigateur RRC. Les privilèges permettant d'autoriser ou de refuser l'accès au port série peuvent être définis dans les menus d'administration (reportez-vous au **Chapitre 4**).

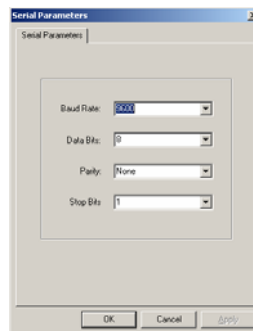


Une fenêtre de terminal dans laquelle figure la sortie console du dispositif série connecté à IP-Reach s'affiche alors et l'icône située à côté de l'entrée du port série dans le navigateur RRC prend la couleur verte.

Remarque : l'accès aux consoles série d'IP-Reach prend uniquement en charge l'émulation de terminal VT100. Avant de procéder à la connexion à IP-Reach, veuillez à ce que votre dispositif série soit correctement configuré.

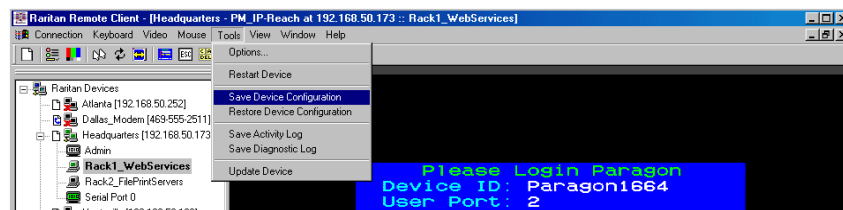
Modification des paramètres série

Vous pouvez modifier les paramètres de terminal série utilisés par IP-Reach pour communiquer avec votre dispositif série (débit en bauds, parité, bits d'arrêt, etc.) en cliquant avec le bouton droit de la souris sur l'entrée du port série dans le navigateur RRC et en sélectionnant **Serial Parameters (Paramètres série)** dans le menu. Cliquez sur [OK] lorsque vous avez terminé.



Administration à distance du dispositif

Lorsque vous êtes connecté à l'unité IP-Reach en tant qu'utilisateur disposant de droits d'administrateur, IP-Reach vous permet d'effectuer à distance de nombreuses tâches d'administration du dispositif.



Menus de configuration

Les utilisateurs disposant de droits d'administrateur peuvent accéder aux menus de configuration de plus faible niveau d'IP-Reach (détaillés au **Chapitre 4**) en double-cliquant sur l'entrée du port « Admin » d'un dispositif IP-Reach figurant dans le navigateur RRC.

Mise à niveau de firmware

Les mises à niveau de firmware peuvent être réalisées à distance en sélectionnant **Tools (Outils) → Update Device (Mettre à jour le dispositif)** dans la barre de menus RRC. RRC vous demande de localiser le fichier de distribution du firmware Raritan (format *.RFP), que vous pouvez trouver, s'il est disponible, sur le site Web de Raritan (www.raritan.com). Veuillez à lire toutes les instructions fournies avec les distributions des firmware avant de procéder à la mise à niveau.

Redémarrage du dispositif

Les utilisateurs disposant de droits d'administrateur peuvent redémarrer les unités IP-Reach en sélectionnant **Tools (Outils) → Restart Device (Redémarrer le dispositif)** dans la barre de menus RRC.

Sauvegarde et restauration de la configuration du dispositif

Les utilisateurs disposant de droits d'administrateur peuvent télécharger des configurations IP-Reach complètes vers ou depuis leurs ordinateurs locaux en vue de l'archivage en sélectionnant **Tools (Outils) → Save Device Configuration (Enregistrer la configuration du dispositif)** et **Tools (Outils) → Restore Device Configuration (Restaurer la configuration du dispositif)** dans la barre de menus RRC.

Fichiers journaux

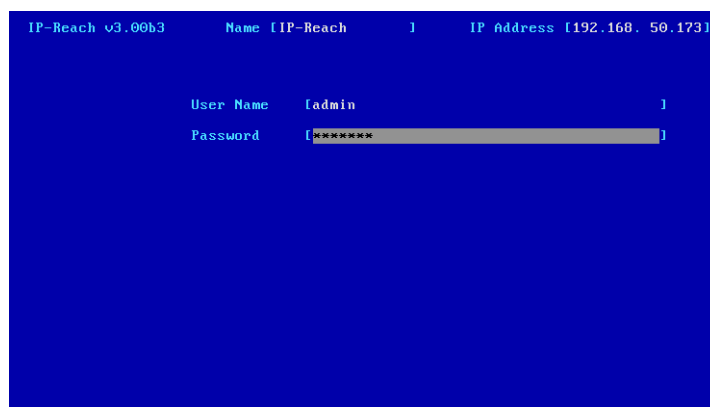
IP-Reach propose des journaux d'activité détaillés à des fins de dépannage. Ces journaux peuvent être téléchargés vers votre ordinateur local et être utilisés ensuite dans le cadre de l'affichage, de la création de rapports et de l'analyse. Dans la barre de menus RRC, sélectionnez **Tools (Outils) → Save Activity Log (Enregistrer le journal d'activité)** ou **Tools (Outils) → Save Diagnostic Log (Enregistrer le journal de diagnostic)**.

Chapitre 4 : Fonctions d'administration

Accès au fonctions d'administration

Vous pouvez accéder aux fonctions d'administration et les lancer via la console d'administration locale ou l'administration à distance. Les menus d'administration d'IP-Reach sont uniquement accessibles aux administrateurs (utilisateurs disposant de droits d'administrateur).

Console d'administration locale



Mettez l'unité IP-Reach SOUS tension à l'aide de l'interrupteur d'alimentation situé sur la partie arrière de l'unité.

Remarque : le nom d'utilisateur et le mot de passe par défaut de IP-Reach pour la connexion sont respectivement <admin> et <raritan>. Si vous vous connectez sous ce nom d'utilisateur et ce mot de passe, vous disposez des droits d'administrateur.

Les mots de passe sont sensibles à la casse, ils doivent être saisis exactement de la même manière que lors de leur création. Le mot de passe par défaut <raritan> doit être saisi uniquement en lettres minuscules.

Pour garantir la sécurité du système, modifiez le nom d'utilisateur et le mot de passe par défaut dès que possible.

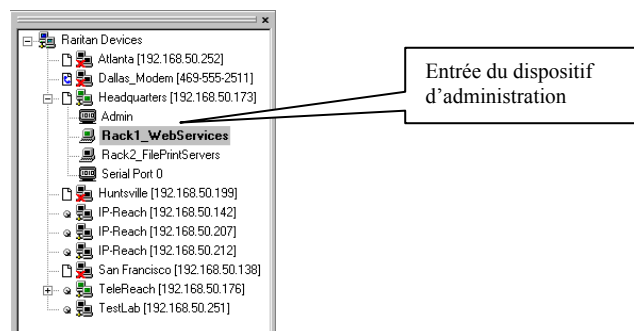
Console d'administration distante

Vous pouvez également accéder aux fonctions d'administration d'IP-Reach à distance, à l'aide de Raritan Remote Client.

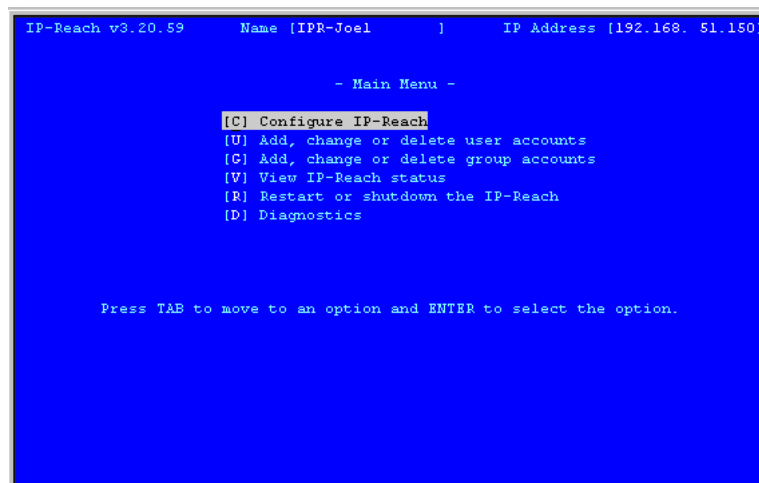
Tous les utilisateurs disposant de droits d'administrateur connectés à IP-Reach depuis un ordinateur distant peuvent lancer à distance des fonctions d'administration permettant d'apporter des modifications au système dans la mesure où IP-Reach est configuré de manière à autoriser les droits d'administrateur distants (reportez-vous à l'option Allow Remote Administration (Autoriser l'administration à distance) de l'écran Security Configuration (Configuration de la sécurité)).

Remarque : seuls les utilisateurs disposant de droits d'administrateur peuvent accéder à la fonction d'administration à distance.

Pour accéder aux menus d'administration à partir de Raritan Remote Client, double-cliquez sur l'entrée du dispositif d'administration du navigateur RRC correspondant à l'unité IP-Reach que vous souhaitez configurer.



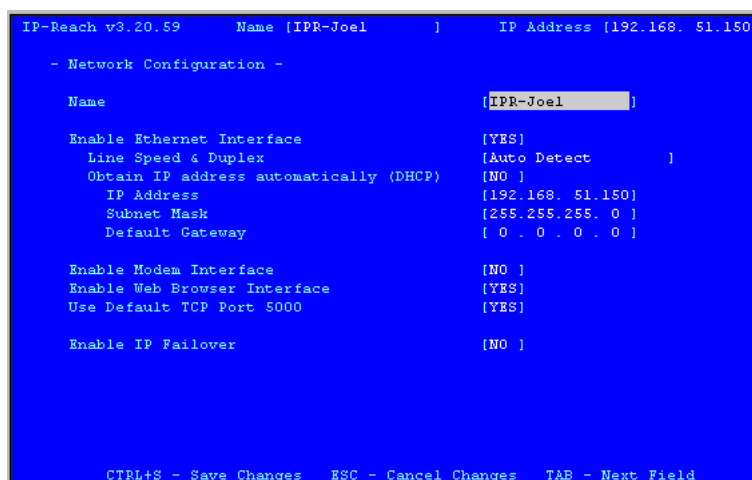
Navigation dans les menus d'administration



- Mettez la sélection Configure IP-Reach (Configurer IP-Reach) en surbrillance à l'aide de la touche <Tabulation>, <↑>, <↓> ou <C> et appuyez sur la touche <Entrée>. Il est possible que vous deviez procéder à un redémarrage.
- Appuyez sur <Ctrl+S> pour enregistrer les modifications.
- Mettez la sélection Network Configuration (Configuration réseau) en surbrillance à l'aide de la touche <Tabulation>, <↑>, <↓> ou <N> et appuyez sur la touche <Entrée>.

Configuration réseau

Une fois la configuration réseau modifiée, appuyez sur <Ctrl+S> pour enregistrer les modifications. Une fois toutes les modifications effectuées, vous devez procéder à un redémarrage pour activer les nouveaux paramètres.



- **Name (Nom)** : indique le nom (unique) de l'unité IP-Reach, « Centre de données de Miami », par exemple. Le nom par défaut est IP-Reach.
- **Enable Ethernet Interface (Activer l'interface Ethernet)** : indique si IP-Reach doit activer son adaptateur Ethernet (valeur par défaut, YES (OUI)).

Remarque : les connexions réseau doivent être de type Ethernet 10BASE-T ou 100BASE-TX.

- **Line Speed & Duplex (Vitesse de ligne & Duplex)** : Auto detect 10 Mbps/Full Duplex (Détection automatique 10 Mbps/Full Duplex), 10 Mbps/Half Duplex, 100 Mbps/Full Duplex ou 100 Mbps/Half Duplex.
- **Obtain IP address automatically (DHCP) (Obtenir l'adresse IP automatiquement (DHCP))** :
 - ♦ **YES (OUI)** : l'adressage IP dynamique d'IP-Reach est activé. A chaque redémarrage, IP-Reach demande une adresse IP auprès du serveur DHCP local. Notez que ce paramètre peut rendre l'accès à distance à IP-Reach difficile hors du réseau local. En effet, pour initier une connexion, l'adresse IP affectée de manière dynamique doit être connue.
 - ♦ **NO (NON) (valeur par défaut)** : une adresse IP fixe est attribuée à l'unité IP-Reach (recommandé).
 - **IP Address (Adresse IP)** : saisissez l'adresse IP que votre administrateur réseau vous a donnée pour IP-Reach.
 - **Subnet Mask (Masque de sous-réseau)** : saisissez le masque de sous-réseau fourni par votre administrateur réseau.
 - **Default Gateway (Passerelle par défaut)** : saisissez la passerelle par défaut indiquée par votre administrateur réseau (le cas échéant).
- **Enable Modem Interface (Activer l'interface modem)** : le modem d'accès à distance est activé (valeur par défaut : YES (OUI)). Sur les modèles IP-Reach M Series, il est nécessaire qu'un modem série externe soit connecté pour que le fonctionnement de ce paramètre soit garanti (reportez-vous au **Chapitre 2 : Installation, Connexions physiques M Series, Port modem dédié**).
- **Enable Web Browser Interface (Activer l'interface du navigateur Web)** : l'accès à IP-Reach via le navigateur Web est activé (valeur par défaut : YES (OUI)).
- **Use Default TCP Port 5000 (Utiliser le port TCP 5000 par défaut)** :
 - **YES (OUI)** (valeur par défaut) : le port TCP 5000 par défaut est utilisé.
 - **NO (NON)** : saisissez le numéro du port que vous souhaitez utiliser à la place.

Remarque : si vous souhaitez accéder à IP-Reach sans l'aide d'un pare-feu, les paramètres que vous définissez pour le pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut (et non du port personnalisé configuré ci-dessus).

- **Enable IP Failover (Activer le basculement IP) (modèles TR Series uniquement)** : ce paramètre, uniquement disponible pour les modèles TR Series, permet d'activer le port Ethernet secondaire en cas de défaillance.
 - Lorsque ce paramètre est activé, IP-Reach vérifie la disponibilité de son port Ethernet primaire selon un intervalle constant, indiqué par le paramètre **Ping Interval in seconds (Intervalle Ping en secondes)**.
 - Lors des vérifications ping, effectuées à intervalles réguliers, si le port Ethernet n'est pas disponible pendant un délai supérieur à celui indiqué par le paramètre **Failover Timeout in seconds (Délai de défaillance en secondes)**, IP-Reach désactive automatiquement son port Ethernet primaire et active son port Ethernet secondaire.

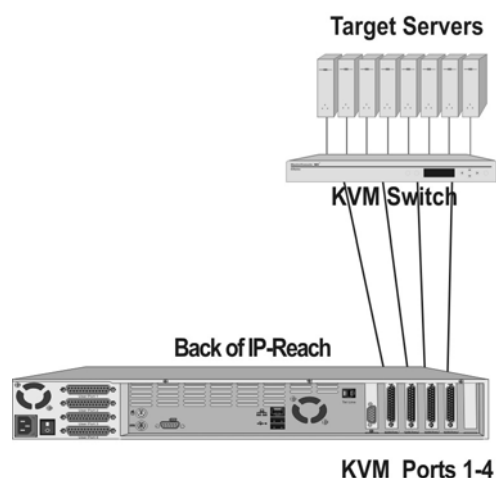
Configuration du chemin

Dans le menu principal, sélectionnez **Configuration → Path Configuration (Configuration du chemin)** pour attribuer un nom aux différents ports d'entrée KVM et pour demander aux modèles IP-Reach disposant de plusieurs ports de rediriger les nouvelles sessions de manière intelligente, en fonction de votre configuration. Si, par exemple, tous les ports d'entrée KVM d'un modèle IP-Reach disposant de plusieurs ports sont connectés au même switch KVM à utilisateurs multiples, IP-Reach peut rediriger automatiquement les sessions entrantes vers un des ports KVM disponibles, tous les ports étant reliés au même switch KVM.

Reportez-vous aux schémas suivants pour déterminer la valeur Path Configuration (Configuration du chemin) adaptée à votre configuration.

Un chemin vers tous les ports :

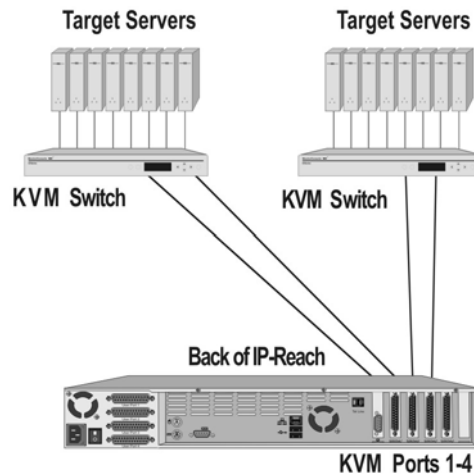
Valeur utilisée lorsque TOUS les ports KVM d'IP-Reach sont connectés à une configuration de switch KVM unique. Il existe un chemin principal vers la configuration KVM unique et quatre utilisateurs au maximum peuvent se connecter à la configuration KVM. IP-Reach affecte automatiquement aux utilisateurs le canal disponible suivant sur le chemin.



Un chemin vers tous les ports

Deux chemins - deux ports chacun :

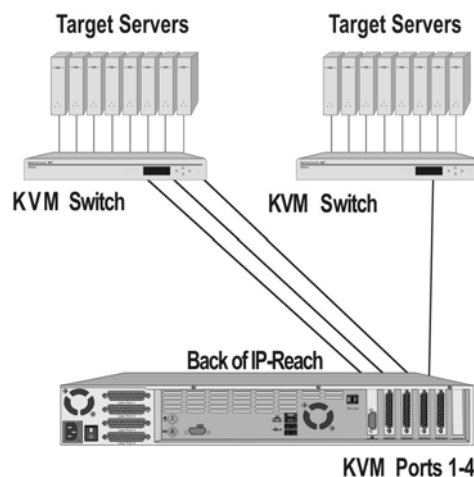
Valeur utilisée lorsqu'IP-Reach est connecté à deux configurations de switch KVM. Il existe deux chemins principaux, un pour chaque configuration KVM. Les utilisateurs doivent sélectionner le chemin (ou la configuration KVM) auquel ils souhaitent accéder lors de l'ouverture de la session IP-Reach. Deux utilisateurs au maximum peuvent se connecter à chaque configuration KVM. IP-Reach affecte automatiquement aux utilisateurs le canal disponible suivant sur le chemin sélectionné.



Deux chemins, deux ports chacun

Deux chemins - trois ports, un port (3,1) :

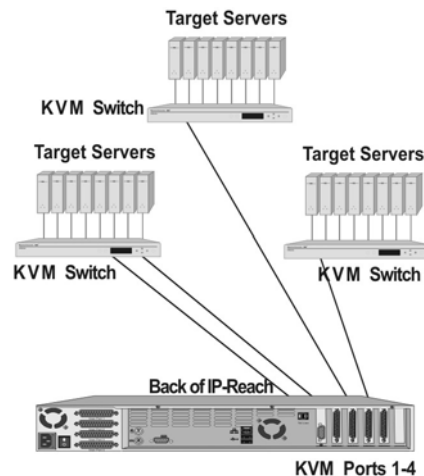
Les utilisateurs doivent sélectionner le chemin (ou la configuration KVM) auquel ils souhaitent accéder lors de l'ouverture de la session IP-Reach. Trois utilisateurs au maximum peuvent se connecter au premier chemin (ou à la première configuration KVM). IP-Reach affecte ensuite automatiquement aux utilisateurs le canal disponible suivant sur le chemin sélectionné. Seul un utilisateur peut se connecter au deuxième chemin (ou à la deuxième configuration KVM).



Deux chemins, trois ports et un port

Trois chemins - deux ports, un port, un port (2, 1, 1) :

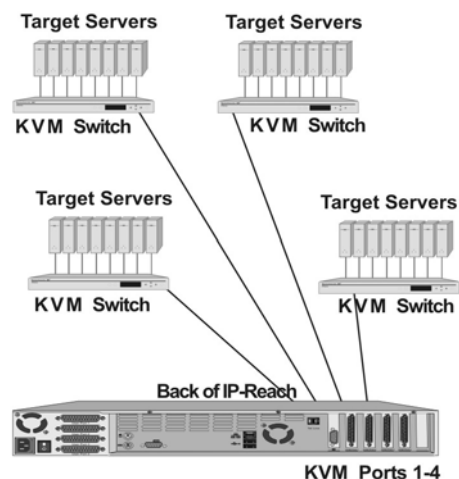
Valeur utilisée lorsqu'IP-Reach est connecté à trois configurations de switch KVM. Il existe trois chemins principaux, un pour chaque configuration KVM. Les utilisateurs doivent sélectionner le chemin (ou la configuration KVM) auquel ils souhaitent accéder lors de l'ouverture de la session IP-Reach. Deux utilisateurs au maximum peuvent se connecter au premier chemin (ou à la première configuration KVM). IP-Reach affecte ensuite automatiquement aux utilisateurs le canal disponible suivant sur le chemin sélectionné. Seul un utilisateur peut se connecter à chacun des chemins restants (ou à chacune des configurations KVM restantes).



Trois chemins, deux ports, un port et un port

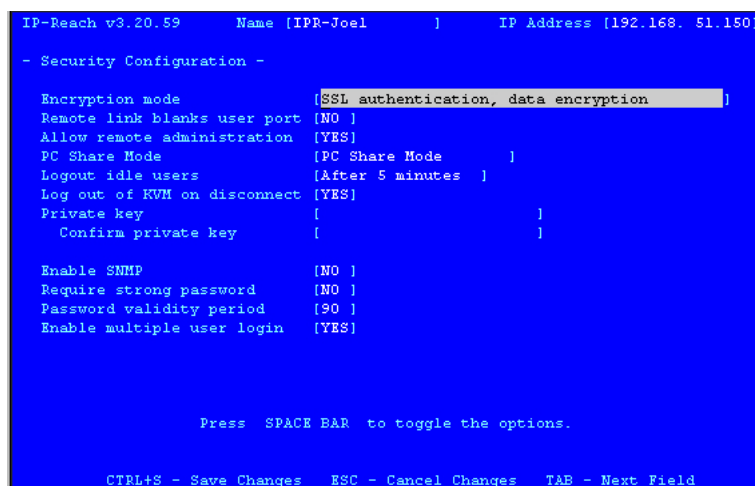
Quatre chemins :

Valeur utilisée lorsqu'IP-Reach est connecté à quatre configurations de switch KVM ou serveurs individuels. Il existe quatre chemins principaux, un pour chaque configuration KVM ou serveur. Les utilisateurs doivent sélectionner le chemin (ou la configuration KVM) auquel ils souhaitent accéder lors de l'ouverture de la session IP-Reach. Seul un utilisateur peut se connecter à chacun des chemins (ou à chacune des configurations KVM).



Quatre chemins - un port pour chaque chemin

Configuration de la sécurité



- **Encryption mode (Mode de cryptage) :** parcourez les différentes options possibles et sélectionnez le niveau de cryptage souhaité pour l'authentification de la connexion initiale et le transfert de données vidéo de la session à distance.
 - **No encryption (Pas de cryptage) :** pas de cryptage ou de sécurité. L'authentification de la connexion initiale et le transfert de données vidéo à distance ne sont pas cryptés.
 - **SSL authentication, NO data encryption (Authentification SSL, PAS de cryptage des données) :** ce mode permet de sécuriser les noms d'utilisateur et les mots de passe, mais pas les données KVM. Le protocole Secure Socket Layer (SSL) 128 bits permet la création d'un canal de communication privé entre IP-Reach et l'ordinateur distant lors de l'authentification de la connexion initiale. Aucune sécurité de cryptage n'est appliquée lors du transfert de données KVM distantes.
 - **SSL authentication, data encryption (Authentification SSL, cryptage des données) (valeur par défaut) :** ce mode permet de sécuriser les noms d'utilisateur, les mots de passe et les données KVM. Le protocole Secure Socket Layer (SSL) 128 bits permet la création d'un canal de communication privé entre IP-Reach et l'ordinateur distant lors de l'authentification de la connexion initiale. Après authentification, les données KVM sont également transmises avec un cryptage 128 bits mais à l'aide d'un protocole propriétaire bien plus efficace que le protocole SSL.
 - **SSL authentication, SSL data encryption (Authentification SSL, cryptage des données SSL) :** ce mode permet de sécuriser les noms d'utilisateur et les mots de passe et d'assurer une sécurité des données KVM de niveau élevé. Le protocole Secure Socket Layer (SSL) 128 bits permet la création d'un canal de communication privé entre IP-Reach et l'ordinateur distant lors de l'authentification de la connexion initiale. Le cryptage SSL 128 bits est également appliqué lors du transfert des données KVM distantes.

Remarque : le cryptage des données SSL augmente la quantité de données devant être expédiées via la connexion à distance, il n'est donc pas recommandé pour les connexions à l'aide d'un modem ou les connexions Internet très lentes. Le paramètre par défaut « SSL authentication, data encryption » (Authentification SSL, cryptage des données) offre le même niveau de sécurité avec un plus haut degré d'efficacité.

- **Remote link blanks user port (le lien distant masque le port utilisateur) :** indique si le port utilisateur analogique direct doit être masqué localement lorsqu'un utilisateur distant accède au port KVM correspondant. Cette option permet d'éviter que les utilisateurs locaux ne voient ce que font les utilisateurs distants.
 - **NO (NON) (valeur par défaut) :** le port utilisateur peut être consulté localement lors de l'accès d'un utilisateur distant.
 - **YES (OUI) :** le port utilisateur ne peut être consulté localement lors de l'accès d'un utilisateur distant. La console utilisateur analogique directe ou locale interrompt l'affichage vidéo.

Remarque : il est possible de relier les consoles utilisateur aux ports 1 à 4. Chaque console utilisateur affiche le chemin du port KVM correspondant. La console utilisateur relié au port utilisateur 1, par exemple, affiche le chemin KVM relié au port KVM 1. De même, la console utilisateur relié au port utilisateur 2 affiche le chemin KVM relié au port KVM 2, etc.

- **Allow remote administration (Autoriser l'administration à distance) :**
 - **NO (NON) :** l'accès à l'ensemble des fonctions administratives est uniquement possible à partir de la console d'administration d'IP-Reach, et non à partir d'un ordinateur distant.
 - **YES (OUI) (valeur par défaut) :** l'accès à distance à l'ensemble des fonctions administratives est possible pour tous les administrateurs connectés sur un ordinateur distant. **Veillez vous référer au Chapitre 3 : Raritan Remote Client, Administration à distance du dispositif pour toute information supplémentaire.**
- **PC Share Mode (Mode PC-Share) :** définit l'accès distant simultané global. Permet à huit utilisateurs au maximum de se connecter simultanément à une unité IP-Reach et d'afficher et de contrôler un serveur cible par l'intermédiaire d'IP-Reach. Le contrôle est basé sur la première saisie de souris/clavier active. Il est donc possible que, si plusieurs utilisateurs distants effectuent une saisie au clavier ou déplacent la souris au même moment, le contrôle soit inégal.
 - **Private Mode (Mode privé) (par défaut) :** aucun partage entre ordinateurs. Seul un utilisateur à la fois peut accéder au chemin IP-Reach.
 - **PC Share Mode (Mode PC-Share) :** plusieurs utilisateurs (administrateurs ou non) peuvent accéder simultanément à IP-Reach. Le contrôle est basé sur la première saisie de souris/clavier active. Il est donc possible que, si plusieurs utilisateurs distants effectuent une saisie au clavier ou déplacent la souris au même moment, le contrôle soit inégal.
 - **PC Share Admins Only (PC-Share administrateurs uniquement) :** plusieurs utilisateurs (administrateurs uniquement) peuvent accéder simultanément à IP-Reach. Le contrôle est basé sur la première saisie de souris/clavier active. Il est donc possible que, si plusieurs utilisateurs distants effectuent une saisie au clavier ou déplacent la souris au même moment, le contrôle soit inégal.

***Remarque :** le paramètre PC Share Mode (Mode PC-Share) est un paramètre global. Pour les paramètres relatifs à l'accès des utilisateurs individuels, reportez-vous aux paramètres Keyboard et Mouse Control (Contrôle de la souris et du clavier) et Concurrent Access Mode (Mode d'accès simultané) de l'écran User Account Settings (Paramètres des comptes utilisateur). Les profils des utilisateurs peuvent être définis individuellement de manière à activer ou désactiver le contrôle de la souris et du clavier et l'accès simultané.*

- **Logout idle users (Déconnexion des utilisateurs inactifs) :** permet à IP-Reach de déconnecter automatiquement les utilisateurs distants à l'issue d'intervalles de temps définis.
 - **Never (Jamais) (valeur par défaut) :** les utilisateurs distants inactifs ne sont jamais déconnectés.
 - **After 5, 15, 30, 60, or 120 minutes (Après 5, 15, 30, 60 ou 120 minutes) :** les utilisateurs distants inactifs sont automatiquement déconnectés d'IP-Reach à l'issue de la période d'inactivité définie pour l'ordinateur distant.
- **Log out of KVM on disconnect (Déconnexion du KVM lors de la déconnexion) :** active la déconnexion automatique de l'affichage à l'écran du KVM connecté.
 - **NO (NON) (valeur par défaut) :** aucune commande spécifique n'est envoyée à l'affichage à l'écran du switch KVM connecté lorsque l'utilisateur distant se déconnecte d'IP-Reach. Lors de la déconnexion de l'utilisateur distant, l'affichage à l'écran du switch KVM connecté reste sur l'écran affiché en dernier à l'utilisateur.
 - **YES (OUI) :** lorsqu'un utilisateur distant se déconnecte d'IP-Reach, IP-Reach envoie automatiquement une commande de déconnexion (<F9>) au switch KVM connecté.

***Remarque :** en cas de connexions multiples, la commande de déconnexion est envoyée, le cas échéant, lorsque le dernier utilisateur connecté se déconnecte d'IP-Reach.*

***Remarque :** pour garantir le fonctionnement correct de l'option de déconnexion du KVM, vous devez configurer IP-Reach conformément au raccourci-clavier du switch KVM de base (reportez-vous au Chapitre 3 : Raritan Remote Client, Administration à distance du dispositif).*

- **Restrict remote IP address (Limiter les adresses IP distantes) :** indique quels emplacements d'adresses IP distantes peuvent accéder à IP-Reach.
 - **NO (NON) (valeur par défaut) :** l'accès à distance à IP-Reach n'est pas limité.
 - **YES (OUI) :** IP-Reach autorise un accès à distance à quatre adresses IP ou niveaux d'adresses IP au maximum. Les administrateurs peuvent configurer IP-Reach de manière à ce que seules les requêtes émises par l'intranet de l'entreprise et/ou par quelques adresses IP extérieures soient autorisées. Les champs IP Mask (Masque IP) indiquent à quelles adresses IP distantes IP-Reach accorde un accès à distance.
 - ♦ Un masque IP spécifique permet de demander à IP-Reach d'accorder uniquement un accès à distance à l'adresse IP distante spécifique donnée. Le masque 10.0.0.1, par exemple, permet

de demander à IP-Reach d'accorder uniquement un accès à distance pour l'emplacement d'adresse IP distante 10.0.0.1.

- ♦ La valeur 255 sert de valeur de remplacement dans les emplacements d'adresses de masque IP. Le masque 10.0.0.255, par exemple, permet de demander à IP-Reach d'accorder un accès à distance pour les emplacements d'adresses IP distantes compris entre 10.0.0.0 et 10.0.0.255. De même, le masque 192.255.255.255 permet de demander à IP-Reach d'accorder un accès à distance pour les emplacements d'adresses IP distantes commençant par 192.

Remarque : une fois que la fonction de limitation des adresses IP distantes est activée, il est nécessaire de saisir un élément dans au moins un des champs IP Mask (Masque IP). En effet, 0.0.0.0 n'est pas une adresse IP valable.

- **Private key (Clé privée) :** saisissez un mot de passe pour la clé privée. Cette clé privée sert de second niveau de protection pour le mot de passe. Seuls les utilisateurs distants qui connaissent le mot de passe de la clé privée, en plus de leurs nom d'utilisateur et mot de passe, peuvent se connecter à IP-Reach.
 - **Confirm private key (Confirmer la clé privée) :** saisissez à nouveau le mot de passe de la clé privée pour confirmation.

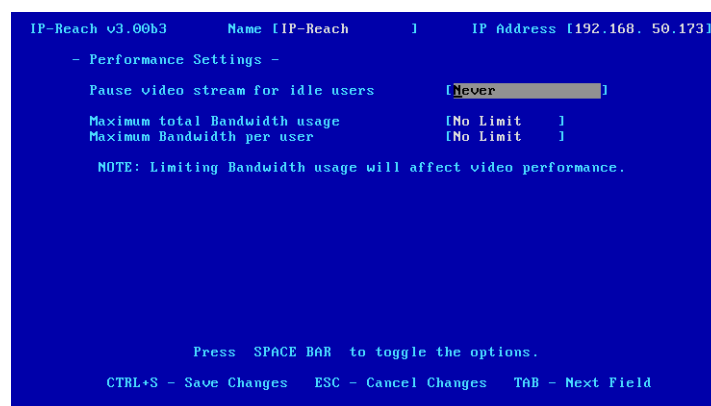
Remarque : les mots de passe des clés privées sont sensibles à la casse. Pour la connexion des utilisateurs distants, les mots de passe doivent être saisis par l'utilisateur avec la même combinaison de casse avec laquelle ils ont été créés.

Remarque : les mots de passe des clés privées doivent être composés de caractères alphanumériques. Les caractères spéciaux ne peuvent être utilisés.

- **Enable SNMP (Activer SNMP) :** indique si IP-Reach doit répondre aux DEMANDES GET SNMP.
- **Require strong password (Mot de passe sécurisé obligatoire) :** les mots de passe des utilisateurs doivent comporter un minimum de 6 caractères avec au moins un caractère alphabétique et un caractère non alphabétique (signe de ponctuation ou chiffre). Les quatre premiers caractères du mot de passe et du nom d'utilisateur ne peuvent être identiques.
- **Password validity period (Période de validité du mot de passe) :** indiquez un nombre de jours dans ce champ afin de forcer les utilisateurs à modifier leur mot de passe à l'issue d'un délai défini.
- **Enable multiple user login (Autoriser la connexion de plusieurs utilisateurs) :** si cette règle est sélectionnée, une combinaison nom d'utilisateur/mot de passe donnée peut être connectée à IP-Reach à partir de plusieurs postes de travail client à la fois.

Paramètres des performances

L'écran Performance Settings (Paramètres des performances) permet de configurer les paramètres relatifs à la bande passante et au transfert de données vidéo d'IP-Reach.



- **Pause video stream for idle users (Interrompre le flux vidéo des utilisateurs inactifs) :** l'interruption du flux de données vidéo lors de périodes d'inactivité prolongée permet d'éviter que la bande passante ne soit utilisée de manière inutile par les utilisateurs inactifs.
 - **Never (Jamais) (valeur par défaut) :** le flux de données vidéo envoyées à l'ordinateur distant n'est jamais interrompu. L'écran est régulièrement mis à jour, même si l'utilisateur distant est inactif. Aucune commande d'inactivité n'est envoyée à IP-Reach.

- **After 5, 15, 30, 60, or 120 minutes (Après 5, 15, 30, 60 ou 120 minutes) :** le flux de données vidéo envoyées à l'ordinateur distant est interrompu à l'issue de la période d'inactivité définie pour l'ordinateur distant.
- **Maximum total Bandwidth usage (Utilisation totale maximale de la bande passante) :** définit la limite supérieure d'utilisation de la bande passante par cette unité IP-Reach.
 - **No Limit (Aucune limite) (valeur par défaut) :** IP-Reach peut utiliser autant de bande passante que nécessaire.
 - **10, 5, 2, or 1 megabit (10, 5, 2 ou 1 mégabit(s)) ou 512, 256, 128 kilobit (512, 256 ou 128 kilobits) :** la quantité totale de bande passante que peut utiliser cette unité IP-Reach est limitée à la quantité sélectionnée. Plus la quantité de bande passante autorisée est faible, plus les performances résultantes risquent d'être lentes.
- **Maximum Bandwidth per user (Bande passante maximale par utilisateur) :** définit la limite supérieure d'utilisation de la bande passante pour chaque utilisateur connecté à cette unité IP-Reach.

***Remarque :** la disponibilité de l'accès distant simultané est déterminée par le paramètre global PC Share Mode (Mode PC-Share) de l'écran Security Configuration (Configuration de la sécurité) ou par chacun des profils utilisateur définis à l'aide des paramètres Keyboard and Mouse Control (Contrôle de la souris et du clavier) et Concurrent Access Mode (Mode d'accès simultané) de l'écran User Account Settings (Paramètres des comptes utilisateur). Le contrôle d'IP-Reach et d'un serveur cible connecté est basé sur la première saisie de souris/clavier active. Il est donc possible que, si plusieurs utilisateurs distants effectuent une saisie au clavier ou déplacent la souris au même moment, le contrôle soit inégal.*

- **No Limit (Aucune limite) (valeur par défaut) :** tous les utilisateurs **actifs** peuvent utiliser autant de bande passante que nécessaire.
- **10, 5, 2, or 1 megabit (10, 5, 2 ou 1 mégabit(s)) ou 512, 256, 128 kilobit (512, 256 ou 128 kilobits) :** la quantité de bande passante utilisée par chacun des utilisateurs actifs lors du **fonctionnement** de cette unité IP-Reach est limitée à la quantité sélectionnée. Plus la quantité de bande passante autorisée est faible, plus les performances résultantes risquent d'être lentes.

Appuyez sur <Ctrl+S> pour enregistrer les modifications ou sur <Echap> pour annuler les modifications et retourner au menu de configuration. Les modifications au niveau des paramètres de performances n'entrent en vigueur qu'après le redémarrage d'IP-Reach.

Important : les informations des deux prochaines sections, *Authentification à distance : utilisateurs, groupes et autorisations d'accès* et *Mise en application d'une authentification à distance* ont subi d'importantes modifications depuis la version 3.1. Veuillez lire attentivement ces sections.

Authentification à distance : utilisateurs, groupes et autorisations d'accès

Présentation

IP-Reach conserve une liste interne des noms des utilisateurs et des groupes pour déterminer l'autorisation d'accès et les autorisations. Ces informations sont stockées de manière interne à l'aide d'un format haché/crypté.

Remarque à l'intention des utilisateurs de CommandCenter

Si vous envisagez de configurer IP-Reach de manière à ce qu'il soit intégré à et contrôlé par l'application de gestion CommandCenter de Raritan, cette section du manuel d'utilisation ne s'applique pas à vous. Si l'unité IP-Reach est contrôlée par CommandCenter, CommandCenter détermine les utilisateurs et les groupes autorisés. Consultez votre guide d'utilisation CommandCenter.

Remarque à l'intention des clients Raritan qui procèdent à une mise à niveau à partir de versions antérieures du firmware

Si vous avez déjà configuré des produits Raritan tels que Dominion KSX et IP-Reach exécutant des versions de firmware propriétaires antérieures à la version 3.2, lisez attentivement l'ensemble de cette section. A compter de la version 3.2 du firmware, la mise en application des utilisateurs et des groupes a changé de manière importante afin de permettre la création de configurations puissantes et plus flexibles.

Relations entre les utilisateurs et les entrées des groupes

IP-Reach répartit l'ensemble des utilisateurs en groupes. La répartition des utilisateurs en groupes vous permet de gérer les autorisations de l'ensemble des utilisateurs d'un groupe donné en une seule fois au lieu de gérer les autorisations utilisateur par utilisateur.

- Les **informations relatives à l'utilisateur** permettent de déterminer l'*authentification* utilisateur (i.e. l'utilisateur est-il autorisé à accéder à IP-Reach ?)
 - Les **informations relatives au groupe** permettent de déterminer l'*autorisation* de l'ensemble des utilisateurs d'un groupe donné (i.e. à quel port d'IP-Reach les utilisateurs du groupe peuvent-ils accéder ?).
- Vous pouvez également choisir de ne pas associer certains utilisateurs à des groupes. L'utilisateur est alors classé par IP-Reach comme « **Individuel** ».

Groupes d'utilisateurs obligatoires

IP-Reach dispose de trois groupes d'utilisateurs par défaut. Ces groupes ne peuvent être supprimés.

ADMIN (ADMINISTRATEUR)	Groupe d'utilisateurs pour l'utilisateur d'administration original par défaut
NONE (AUCUN)	Les autorisations définies pour ce groupe sont utilisées pour les utilisateurs lorsque votre IP-Reach est configuré pour l'authentification à distance par l'intermédiaire de LDAP ou de RADIUS (reportez-vous à la section suivante), que la tentative de connexion se déroule de manière réussie et qu'aucun groupe d'utilisateurs n'est retourné par le serveur d'authentification à distance.
UNKNOWN (INCONNU)	Les autorisations définies pour ce groupe sont utilisées pour les utilisateurs lorsque votre IP-Reach est configuré pour l'authentification à distance par l'intermédiaire de LDAP ou de RADIUS (reportez-vous à la section suivante), que la tentative de connexion se déroule de manière réussie et que le groupe d'utilisateurs retourné par le serveur d'authentification à distance n'est pas localisé au niveau d'IP-Reach.

Création ou modification de comptes groupe

1. Dans le menu principal, saisissez la lettre <G> pour ajouter ou modifier un compte groupe.

```

IP-Reach v3.20.61      Name [IP-Reach_3.2 ]      IP Address [192.168. 51.150]

- Main Menu -

[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.

```

2. L'écran **Group Account (Compte groupe)** s'affiche.
 - a. Pour ajouter un nouveau compte groupe, saisissez la lettre <A>.
 - b. Pour modifier les propriétés d'un compte groupe, utilisez la touche <TABULATION> pour vous déplacer dans la liste et appuyez sur <ENTREE> pour sélectionner le groupe que vous souhaitez modifier.

```

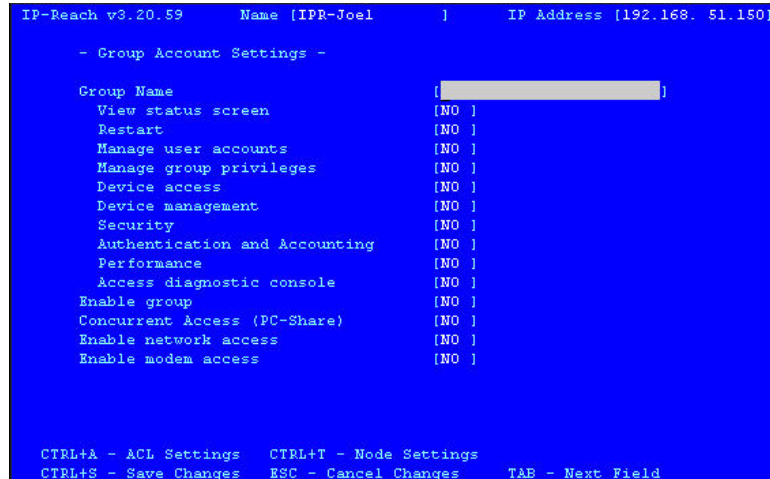
IP-Reach v3.20.59      Name [IPR-Joel ]      IP Address [192.168. 51.150]

Group Account
-----
ADMIN

A - Add a new group  TAB - Next Group  C - Change Group  D - Delete group
ESC - Exit          N - Next page    P - Previous page

```

3. L'écran **Group Account Settings (Paramètres du compte groupe)** s'affiche.
 - a. Saisissez le nom du compte groupe dans le champ **Group Name (Nom du groupe)**. Le nom peut être composé de 23 caractères alphanumériques au maximum. Le premier caractère ne peut pas être un chiffre.
 - b. Utilisez les touches en forme de flèches, <↑> et <↓>, ou la touche <TABULATION> pour vous déplacer entre les éléments des lignes et appuyez sur la touche <BARRE D'ESPACE> pour passer de l'option YES (OUI) à l'option NO (NON). Une fois les modifications effectuées, appuyez sur <CTRL> + <S> pour enregistrer les données ou sur <ECHAP> pour fermer l'écran sans enregistrer les données.

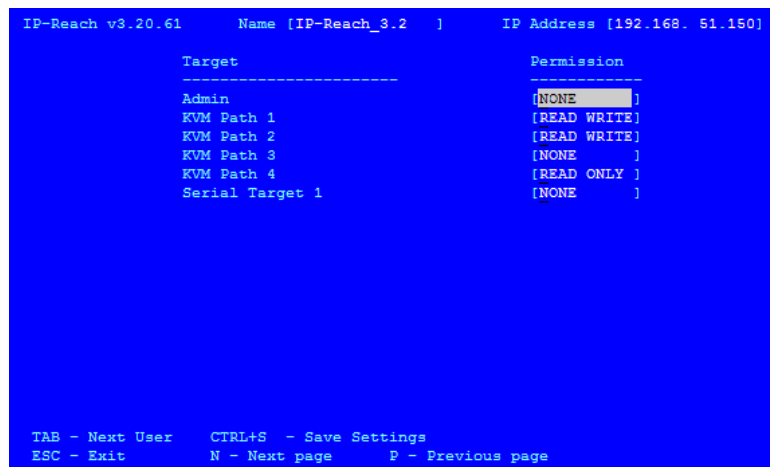


4. Appuyez sur <CTRL> + <S> pour enregistrer les modifications.

Attribution des autorisations d'accès aux ports

Par défaut, les nouveaux groupes d'utilisateurs ne disposent d'aucun droit d'accès aux ports série et KVM d'IP-Reach. Vous devez attribuer des autorisations d'accès aux différents groupes d'utilisateurs.

1. Lorsque l'écran **Group Account Settings (Paramètres du compte groupe)** correspondant à un groupe d'utilisateurs est affiché (lors de la création d'un groupe ou de l'édition d'un nouveau groupe), appuyez sur <CTRL>+<T> pour sélectionner **Node Settings (Paramètres du noeud)**.
2. Le menu **Node Settings (Paramètres du noeud)**, dans lequel l'ensemble des ports série et KVM configurés sur votre IP-Reach est répertorié, s'affiche.



3. Utilisez les touches en forme de flèches, <↑> et <↓>, pour naviguer entre les ports série et KVM configurés sur votre IP-Reach et appuyez sur la touche <BARRE D'ESPACE> pour sélectionner une des options suivantes :
 - a. **NONE (AUCUNE)** - les utilisateurs de ce groupe ne sont pas autorisés à accéder à ce port série ou KVM. Le port n'est même pas affiché comme option disponible pour les utilisateurs de ce groupe.
 - b. **READ ONLY (LECTURE SEULEMENT)** - les utilisateurs de ce groupe peuvent afficher ce port de console série ou KVM mais ne sont pas autorisés à le contrôler (saisie, déplacement de la souris, etc.).
 - c. **READ WRITE (LECTURE/ECRITURE)** - les utilisateurs de ce groupe peuvent afficher ce port de console série ou KVM et sont autorisés à le contrôler.
4. Appuyez sur <CTRL>+<S> pour enregistrer les modifications.

- Les modifications que vous avez apportées ne sont **pas encore enregistrées**. L'écran **Group Account Settings (Paramètres du compte groupe)** correspondant au groupe d'utilisateurs que vous éditez ou créez s'affiche.

```

IP-Reach v3.20.61      Name [IP-Reach_3.2 ]      IP Address [192.168. 51.150]

- Group Account Settings -

Group Name              [Windows Admins ]
View status screen      [YES]
Restart                 [NO ]
Manage user accounts    [NO ]
Manage group privileges [NO ]
Device access           [YES]
Device management       [NO ]
Security                [NO ]
Authentication and Accounting [NO ]
Performance             [NO ]
Access diagnostic console [NO ]
Enable group            [YES]
Concurrent Access (PC-Share) [NO ]
Enable network access   [YES]
Enable modem access     [NO ]

CTRL+A - ACL Settings  CTRL+T - Node Settings
CTRL+S - Save Changes  ESC - Cancel Changes   TAB - Next Field

```

- Appuyez de nouveau sur <CTRL>+<S> lorsque vous vous trouvez dans cet écran pour enregistrer les paramètres d'autorisation du groupe d'utilisateurs donné.

Suppression de comptes groupe

Pour supprimer un compte groupe existant, saisissez la lettre <G> dans le menu principal. Lorsque l'écran Group Account (Compte groupe) s'affiche, appuyez sur <TABULATION> pour sélectionner le compte groupe que vous souhaitez supprimer et appuyez ensuite sur la lettre <D>. Avant de supprimer un groupe, assurez-vous qu'aucun utilisateur n'est affecté au groupe. Les utilisateurs affectés au groupe seront également supprimés.

Veillez noter que vous ne pouvez pas supprimer **ADMIN**, le groupe par défaut.

```

IP-Reach v3.20.59      Name [IPR-Joel ]      IP Address [192.168. 51.150]

Group Account
-----
ADMIN_

A - Add a new group  TAB - Next Group  C - Change Group  D - Delete group
ESC - Exit          N - Next page    P - Previous page

```

Création ou modification de comptes utilisateur

- Dans le menu principal, saisissez la lettre <U> pour ajouter ou modifier un compte utilisateur.

```

IP-Reach v3.20.59      Name [IPR-Joel ]      IP Address [192.168. 51.150]

- Main Menu -

[C] Configure IP-Reach
[U] Add, change or delete user accounts
[C] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.

```

2. La fenêtre **User Account (Compte utilisateur)** s'affiche.
 - a. Pour ajouter un nouveau compte utilisateur, saisissez la lettre **<A>**.
 - b. Pour modifier les propriétés d'un compte utilisateur, utilisez la touche **<TABULATION>** pour vous déplacer dans la liste et appuyez sur **<ENTREE>** pour sélectionner l'utilisateur que vous souhaitez modifier.

```

IP-Reach v3.20.59      Name [IPR-Joel ]      IP Address [192.168. 51.150]

User Account          Logged In
-----
ADMIN                 [YES]
JOEL                  [NO ]
NONE                  [NO ]
UNKNOWN               [NO ]

A - Add a new user    TAB - Next User    C - Change User      D - Delete user
L - Log off a user    ESC - Exit      N - Next page        P - Previous page

```

3. L'écran **User Account Settings (Paramètres du compte utilisateur)** s'affiche.
 - a. Saisissez le nom de l'utilisateur dans le champ **User Name (Nom d'utilisateur)**. Le nom peut être composé de 23 caractères alphanumériques au maximum. Le premier caractère ne peut pas être un chiffre.
 - b. Saisissez le mot de passe de l'utilisateur dans le champ **Password (Mot de passe)**. Le mot de passe peut être composé de 23 caractères alphanumériques au maximum.
 - c. Saisissez de nouveau le mot de passe pour vérification dans le champ **Confirm password (Confirmer le mot de passe)**.
 - d. Dans le champ **Account Enabled (Compte activé)**, appuyez sur la touche **<BARRE D'ESPACE>** pour passer de l'option YES (OUI) à l'option NO (NON) et activer ainsi le compte de cet utilisateur (valeur par défaut : NO (NON)).
 - e. Saisissez le nom du groupe auquel cet utilisateur appartient dans le champ **Group Name (Nom du groupe)**.
 - f. Une fois les modifications effectuées, appuyez sur **<CTRL> + <S>** pour enregistrer vos données ou sur **<ECHAP>** pour fermer l'écran sans enregistrer les données.

```

IP-Reach v3.20.59      Name [IPR-Joel ]      IP Address [192.168. 51.150]

- User Account Settings -

User Name              [          ]
Password               [          ]
Confirm password       [          ]

Account Enabled        [NO ]
Group Name             [          ]

Press SPACE BAR to toggle the options.

CTRL+S - Save Changes  ESC - Cancel Changes  TAB - Next Field

```

4. Appuyez sur **<CTRL> + <M>** pour retourner au menu principal.

Suppression de comptes utilisateur

Pour supprimer un compte utilisateur existant, saisissez la lettre <U> dans le menu principal. Lorsque l'écran User Account (Compte utilisateur) s'affiche, appuyez sur <TABULATION> pour sélectionner le compte utilisateur que vous souhaitez supprimer et appuyez ensuite sur la lettre <D>.

Veillez noter que vous ne pouvez pas supprimer **ADMIN**, l'utilisateur par défaut.

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

      User Account      Logged In
      -----
      ADMIN             [YES]
      JOEL              [NO ]
      NONE              [NO ]
      UNKNOWN          [NO ]

A - Add a new user      TAB - Next User      C - Change User      D - Delete user
L - Log off a user      ESC - Exit      N - Next page      P - Previous page

```

Mise en application d'une authentification à distance

Introduction

Remarque à l'intention des utilisateurs de CommandCenter

Si vous envisagez de configurer IP-Reach de manière à ce qu'il soit intégré à et contrôlé par l'application de gestion CommandCenter de Raritan, cette section du manuel d'utilisation ne s'applique pas à vous. Si l'unité IP-Reach est contrôlée par CommandCenter, CommandCenter détermine les utilisateurs et les groupes autorisés. Consultez votre guide d'utilisation CommandCenter.

Remarque à l'intention des clients Raritan qui procèdent à une mise à niveau à partir de versions antérieures du firmware

Si vous avez déjà mis en application l'authentification RADIUS sur des produits Raritan tels que Dominion KSX et IP-Reach exécutant des versions de firmware propriétaires antérieures à la version 3.2, lisez attentivement l'ensemble de cette section. A compter de la version 3.2 du firmware, la mise en application de l'authentification externe a changé de manière importante afin de permettre la création de configurations puissantes et plus flexibles.

Protocoles pris en charge

Afin de simplifier la gestion des noms des utilisateurs et des mots de passe, il est possible d'utiliser IP-Reach pour transférer les requêtes d'authentification vers un serveur d'authentification externe. IP-Reach prend en charge deux protocoles d'authentification externes : LDAP et RADIUS.

Remarque relative à Microsoft Active Directory

Microsoft Active Directory utilise le protocole LDAP de manière native et peut être utilisé comme source d'authentification et serveur LDAP avec IP-Reach. Si le serveur Microsoft Active Directory dispose d'un composant IAS (serveur d'autorisation Internet), il peut également être utilisé comme source d'authentification RADIUS.

Mise en application d'une authentification à distance

Priorité

Lorsqu'un utilisateur procède à l'authentification auprès d'une unité IP-Reach configurée pour l'authentification externe, IP-Reach vérifie d'abord si le nom de l'utilisateur figure dans sa base de données utilisateur propre. Si le nom de l'utilisateur ne peut être localisé dans la base de données interne d'IP-Reach, la requête est transmise au serveur d'authentification externe.

- **Si le nom de l'utilisateur ne peut être localisé dans la base de données interne d'IP-Reach** : la requête est transmise au serveur d'authentification externe afin de déterminer si la connexion est ou non autorisée.
- **Si le nom de l'utilisateur est localisé dans la base de données interne d'IP-Reach et que le mot de passe est correct** : la connexion est autorisée.
- **Si le nom de l'utilisateur ne peut être localisé dans la base de données interne d'IP-Reach et que le mot de passe n'est pas correct** : la connexion est refusée et la requête n'est PAS transmise au serveur d'authentification externe.

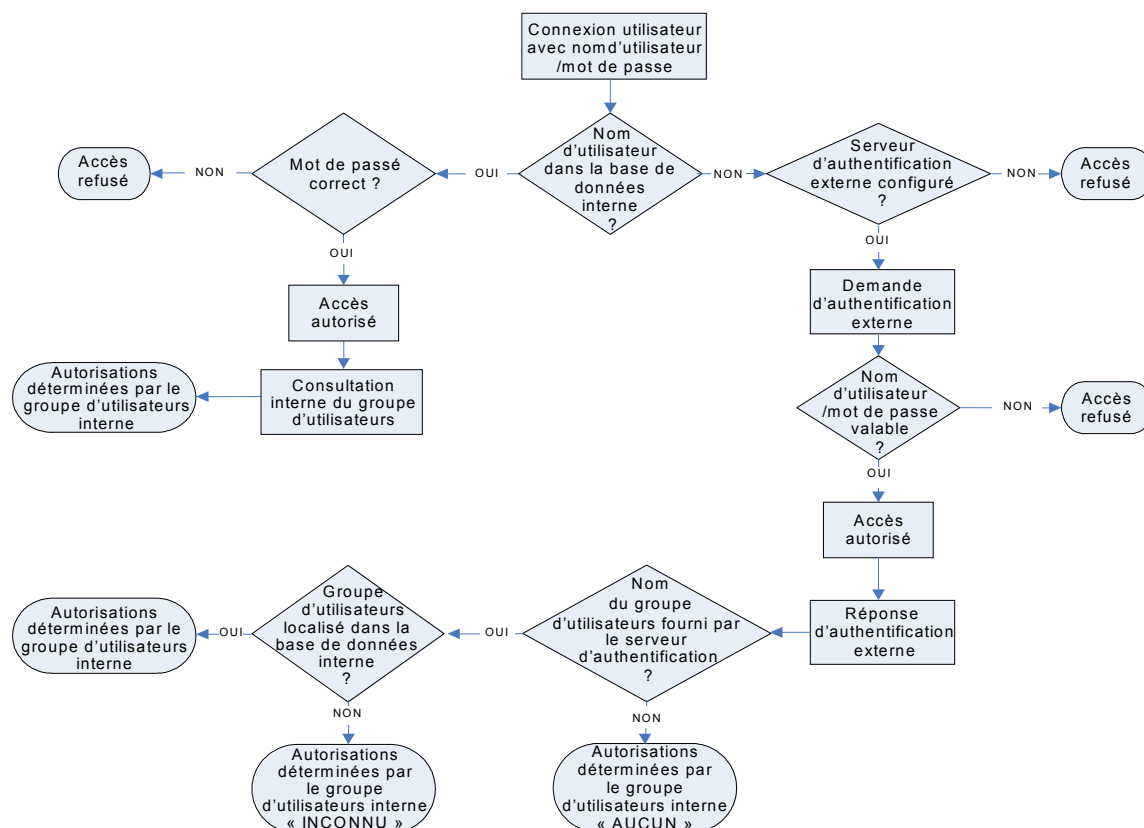
Authentification et autorisation

Si votre unité IP-Reach est configurée de manière à permettre l'authentification à distance, le serveur d'authentification externe est essentiellement utilisé dans un but d'authentification et non d'autorisation.

L'autorisation est déterminée par IP-Reach selon les groupes d'utilisateurs. I.e. une fois qu'un utilisateur donné est autorisé à accéder au système IP-Reach en général (authentifié), l'autorisation spécifique de cet utilisateur est déterminée par IP-Reach selon le groupe auquel appartient l'utilisateur.

Le serveur d'authentification externe peut contribuer à l'autorisation en informant IP-Reach au sujet du groupe d'utilisateurs auquel appartient un utilisateur lorsque le serveur d'authentification approuve la requête de connexion d'un utilisateur donné. Les sections **Mise en application de l'authentification à distance LDAP** et **Mise en application de l'authentification à distance RADIUS** (dans la suite de ce manuel) expliquent ce phénomène plus en détail.

L'organigramme suivant illustre les différentes étapes nécessaires :



Notez l'importance du groupe auquel appartient un utilisateur donné ainsi que la nécessité de configurer les groupes appelés « UNKNOWN » (INCONNU) et « NONE » (AUCUN). Si le serveur d'authentification externe renvoie un nom de groupe qui n'est pas reconnu par IP-Reach, les autorisations de l'utilisateur sont déterminées par le groupe permanent appelé « UNKNOWN » (INCONNU). Si le serveur d'authentification externe ne renvoie aucun nom de groupe, les permissions de l'utilisateur sont déterminées par le groupe permanent appelé « NONE » (AUCUN).

Reportez-vous aux sections **LDAP** et **RADIUS** de ce chapitre pour savoir comment configurer votre serveur d'authentification de manière à ce qu'il renvoie les informations relatives au groupe d'utilisateurs à IP-Reach dans le cadre de sa réponse à une demande d'authentification.

Paramètres généraux pour l'authentification à distance

Pour définir les propriétés d'authentification, vous devez vous connecter à IP-Reach en tant qu'administrateur par défaut (nom d'utilisateur <admin>, mot de passe <raritan>).

1. Dans le menu principal, appuyez sur la lettre <C> pour configurer IP-Reach.

```
IP-Reach v3.20.61      Name [IP-Reach_3.2  ]      IP Address [192.168. 51.150]

- Main Menu -

[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics

Press TAB to move to an option and ENTER to select the option.
```

2. Lorsque le menu de configuration s'affiche, appuyez sur <R> pour configurer l'authentification à distance. L'écran **Authentication and Accounting (Authentification et gestion)** apparaît.

```
IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Authentication and Accounting-

Enable Remote Authentication [NONE ]
Enable Remote Accounting     [NONE ]

Press SPACE BAR to toggle the options.
```

3. Appuyez sur <BARRE D'ESPACE> pour activer les options du protocole d'authentification à distance que vous souhaitez utiliser et sélectionnez RADIUS, LDAP ou LDAPS.

```
IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Authentication and Accounting-

Enable Remote Authentication [RADIUS]
Enable Remote Accounting     [NONE ]

Authentication Type          [CHAP]
Server Secret                [                ]
Confirm Secret               [                ]
Server Timeout (seconds)    [2 ]
Primary Server IP            [0 . 0 . 0 . 0 ]
Secondary Server IP          [0 . 0 . 0 . 0 ]
Server UDP Port              [Standard Port 1812 ]

Press SPACE BAR to toggle the options.
```

4. L'écran Authentication and Accounting (Authentification et gestion) du protocole que vous avez sélectionné apparaît. Déplacez-vous entre les champs à l'aide de la touche <TABULATION>.
 - a. Appuyez sur <BARRE D'ESPACE> pour accéder au champ **Authentication Type (Type d'authentification)**.

- b. Saisissez le secret du serveur nécessaire à l'authentification de vos serveurs d'authentification à distance dans le champ **Server Secret (Secret du serveur)**. Saisissez de nouveau le secret du serveur dans le champ **Confirm Secret (Vérifier le secret)**.
 - c. Dans le champ **Server Timeout (seconds) (Expiration du serveur (en secondes))**, saisissez le délai d'inactivité (en secondes) qui doit s'écouler avant expiration du serveur.
 - d. Saisissez l'adresse IP des serveurs d'authentification à distance principal et secondaire que vous utilisez dans les champs **Primary Server IP (IP du serveur principal)** et **Secondary Server IP (IP du serveur secondaire)**.
5. Si vous avez sélectionné le protocole LDAP comme protocole d'authentification à distance, passez à la section suivante, **Mise en application de l'authentification à distance LDAP**, pour remplir les champs du panneau LDAP de la fenêtre Remote Authentication (Authentification à distance). Si vous avez sélectionné le protocole RADIUS, passez à la section **Mise en application de l'authentification à distance RADIUS** pour remplir les champs du panneau RADIUS de la fenêtre.

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Authentication and Accounting-

Enable Remote Authentication [LDAP ]

Server Secret          [                  ]
Confirm Secret         [                  ]
Server Timeout (seconds) [2 ]
Primary Server IP      [ 0 . 0 . 0 . 0 ]
Secondary Server IP    [ 0 . 0 . 0 . 0 ]
Server Port            [Standard LDAP Port      ]

Base Dn                [                  ]
Base Search             [                  ]

Press SPACE BAR to toggle the options.

```

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Authentication and Accounting-

Enable Remote Authentication [LDAPS ]

Server Secret          [                  ]
Confirm Secret         [                  ]
Server Timeout (seconds) [2 ]
Primary Server IP      [ 0 . 0 . 0 . 0 ]
Secondary Server IP    [ 0 . 0 . 0 . 0 ]
Server Port            [Standard LDAP Port      ]

Base Dn                [                  ]
Base Search             [                  ]

Press SPACE BAR to toggle the options.

```

6. Si vous souhaitez activer la gestion à distance, dans l'écran **Authentication and Accounting (Authentification et gestion)**, accédez au champ **Enable Remote Accounting (Activer la gestion à distance)** à l'aide de la touche <TABULATION> et appuyez sur <BARRE D'ESPACE> pour activer l'option RADIUS.

```

IP-Reach v3.20.59      Name [IPR-Joel      ]      IP Address [192.168. 51.150]

- Authentication and Accounting-

Enable Remote Authentication [NONE ]
Enable Remote Accounting   [RADIUS]

Server Secret          [                  ]
Confirm Secret         [                  ]
Server Timeout (seconds) [2 ]
Primary Server IP      [ 0 . 0 . 0 . 0 ]
Secondary Server IP    [ 0 . 0 . 0 . 0 ]
Server UDP Port        [Standard Port 1813      ]

Press SPACE BAR to toggle the options.

```

7. Une fois les modifications effectuées, appuyez sur <ENTREE> pour enregistrer les modifications ou sur <ECHAP> pour fermer l'écran sans enregistrer la configuration d'authentification à distance.

Mise en application de l'authentification à distance LDAP

Rappel : Microsoft Active Directory fonctionne de manière native comme un serveur d'authentification LDAP.

Si vous choisissez le protocole d'authentification LDAP, remplissez les champs LDAP de la manière suivante :

- **Use Secure LDAP (Utiliser le LDAP sécurisé)** : appliquez cette règle pour activer LDAP-S qui permet de garantir que toutes les requêtes d'authentification et les réponses transmises sur le réseau sont cryptées.
- **Default Port (Port par défaut)/User Defined Port (Port défini par l'utilisateur)** : sélectionnez la case d'option vous permettant d'utiliser les ports TCP LDAP standard ou indiquez un port que vous avez vous-même défini.
- **Base DN (Base DN), Base Search (Recherche de base) et Certificate File (Fichier du certificat)** : consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs afin de traiter les demandes d'authentification LDAP à partir d'IP-Reach.

Renvoi des informations relatives aux groupes d'utilisateurs par l'intermédiaire du LDAP

Lorsque la demande d'authentification LDAP est acceptée, IP-Reach détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel appartient l'utilisateur. Votre serveur LDAP distant peut fournir ces noms de groupes d'utilisateurs en renvoyant un attribut désigné de la manière suivante :

```
rciusergroup          attribute type: string
```

Il est possible que cette opération nécessite une extension de schéma sur votre serveur LDAP. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

Mise en application de l'authentification à distance RADIUS

Si vous installez le composant de serveur Windows **Internet Authentication Server (Serveur d'authentification Internet)**, Microsoft Active Directory peut être utilisé comme source principale pour l'authentification RADIUS.

Si vous choisissez le protocole d'authentification RADIUS, remplissez les champs RADIUS de la manière suivante :

- **Authentication Type (Type d'authentification)** : cliquez sur la flèche de la liste déroulante pour sélectionner le protocole CHAP ou le protocole PAP.
- **Server UDP Port (Port UDP du serveur)/Custom UDP Port (Port UDP personnalisé)** : cliquez sur la flèche de la liste déroulante pour indiquer si vous préférez utiliser le port TCP RADIUS 1812 standard, le port TCP RADIUS 1645 patrimonial ou saisissez le port que vous avez vous-même défini dans le champ **Custom UDP Port (Port UDP personnalisé)**.
- **Remote Accounting (Gestion à distance)/Custom Accounting Port (Port de gestion personnalisé)** : activez la case à cocher pour envoyer les événements d'authentification à un serveur de gestion RADIUS. Si vous activez la case à cocher, vous devez indiquer le port TCP qui doit être utilisé pour la transmission des événements dans le champ **Custom Accounting Port (Port de gestion personnalisé)**.

Renvoi des informations relatives aux groupes d'utilisateurs par l'intermédiaire du RADIUS

Lorsque la demande d'authentification RADIUS est acceptée, IP-Reach détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel appartient l'utilisateur.

Votre serveur RADIUS distant peut fournir ces noms de groupes d'utilisateurs en retournant un attribut, mis en application comme un *FILTER-ID (ID FILTRE)* RADIUS. Le format du *FILTER-ID (ID FILTRE)* doit être le suivant :

Raritan:G{GROUP_NAME}

où GROUP_NAME est une chaîne de caractères indiquant le nom du groupe auquel l'utilisateur appartient.

Spécifications des échanges de communication RADIUS

IP-Reach envoie les informations suivantes au serveur RADIUS dans une demande d'authentification :

ATTRIBUT	DONNEES
USER-NAME (NOM D'UTILISATEUR)	Nom d'utilisateur saisi dans l'écran de connexion
USER-PASSWORD (MOT DE PASSE UTILISATEUR)	En mode PAP, mot de passe crypté saisi dans l'écran de connexion
CHAP-PASSWORD (MOT DE PASSE CHAP)	En mode CHAP, réponse du protocole CHAP obtenue à partir du mot de passe et données relatives à la demande d'accès CHAP
NAS-IP-ADDRESS (ADRESSE IP NAS)	Adresse IP d'IP-Reach
NAS-IDENTIFIER (IDENTIFIANT NAS)	Nom de l'unité IP-Reach configuré dans « Network Configuration » (Configuration réseau) (reportez-vous à la section précédente)
NAS-PORT-TYPE (TYPE DE PORT NAS)	Valeur ASYNC (0) pour les connexions modem et ETHERNET (15) pour les connexions réseau
NAS-PORT (PORT NAS)	Toujours 0
STATE (ETAT)	Si la demande répond à un ACCESS-CHALLENGE (DEMANDE D'ACCES), les données d'état du paquet ACCESS-CHALLENGE (DEMANDE D'ACCES) sont renvoyées.
PROXY-STATE (ETAT DU PROXY)	Si la demande répond à un ACCESS-CHALLENGE (DEMANDE D'ACCES), les données d'état du proxy du paquet ACCESS-CHALLENGE (DEMANDE D'ACCES) sont renvoyées.

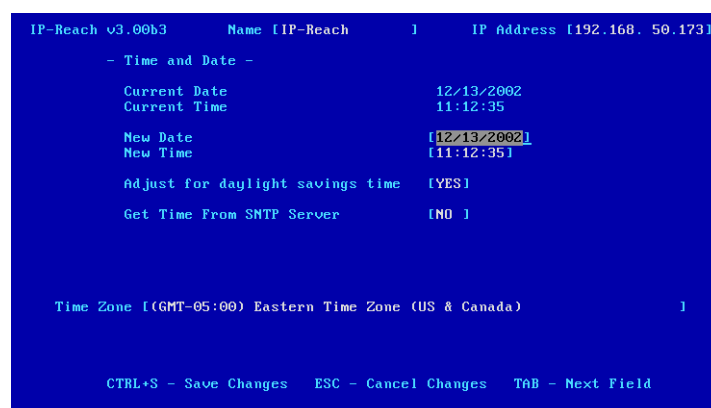
IP-Reach envoie les attributs RADIUS suivants au serveur RADIUS avec chaque requête de gestion :

ATTRIBUT	DONNEES
SESSION-TYPE (TYPE DE SESSION)	START (DEMARRER) (1) pour la connexion ou STOP (ARRETER) (2) pour la déconnexion
SESSION-ID (ID DE SESSION)	Chaîne de caractères comprenant un nom de session unique. Le nom est au format « <IDENTIFICATEUR NAS>:<adresse IP de l'utilisateur>:<numéro de session unique> ». Exemple : « IP-Reach:192.168.1.100:122 »
USER-NAME (NOM D'UTILISATEUR)	Comme ci-dessus
NAS-IP-ADDRESS (ADRESSE IP NAS)	Comme ci-dessus
NAS-IDENTIFIER (IDENTIFIANT NAS)	Comme ci-dessus
NAS-PORT-TYPE (TYPE DE PORT NAS)	Comme ci-dessus
NAS-PORT (PORT NAS)	Comme ci-dessus
FILTER-ID (ID FILTRE)	Les attributs FILTER-ID (ID FILTRE) retournés par le serveur RADIUS lors de l'authentification sont envoyés avec chaque requête de gestion.

ATTRIBUT	DONNEES
CLASS (CLASSE)	Les attributs CLASS (CLASSE) retournés par le serveur RADIUS lors de l'authentification sont envoyés avec chaque requête de gestion.
ACCT-AUTHENTIC (AUTHENTIFICATION CPTE)	Méthode d'authentification de l'utilisateur. RADIUS (1) si l'utilisateur a été authentifié par le serveur RADIUS ou LOCAL (2) si l'utilisateur a été authentifié par la base de données nom d'utilisateur intégrée d'IP-Reach.
TERMINATE-CAUSE (CAUSE DE LA DECONNEXION)	S'il s'agit d'une requête STOP (ARRETER), la raison pour laquelle l'utilisateur a été déconnecté. USER_REQUEST (REQUETE DE L'UTILISATEUR) (1), LOST_SERVICE (PERTE DU SERVICE) (3), SESSION_TIMEOUT (EXPIRATION DE LA SESSION) (5) ou ADMIN_RESET (REINITIALISATION DE L'ADMINISTRATEUR) (6).

Heure et date

L'heure et la date actuellement configurées sur l'unité IP-Reach s'affichent sur cet écran. Une fois enregistrées, les modifications au niveau de la date et de l'heure n'entrent en vigueur qu'après le redémarrage d'IP-Reach.



- **New Date (Nouvelle date)/New Time (Nouvelle heure)** : permettent de modifier manuellement les valeurs sélectionnées pour la date et l'heure.
- **Adjust for daylight savings time (Régler selon les changements d'heure)** : activez l'option YES (OUI) ou NO (NON) selon que votre pays ou votre région respecte ou non les procédures de changement d'heure.
- **Get Time From SNTP Server (Obtenir l'heure à partir du serveur SNTP)** : indique si la date/l'heure d'IP-Reach doit être automatiquement synchronisée sur la date/l'heure d'un serveur SNTP externe.
 - **Primary Server IP Address (Adresse IP du serveur primaire)** : adresse IP du premier serveur SNTP qui tente de procéder à une synchronisation de temps.
 - **Secondary Server IP Address (Adresse IP du serveur secondaire)** : adresse IP du serveur SNTP qui doit être sollicité si le premier serveur n'est pas disponible.
 - **User standard UDP port 123 (Port UDP 123 standard pour utilisateurs)** : permet aux utilisateurs de modifier le port UDP utilisé pour la synchronisation de temps SNTP. Pour savoir si cette valeur doit être réglée, consultez l'administrateur de votre serveur SNTP.
- **Time Zone (Fuseau horaire)** : sélectionnez le fuseau horaire correspondant à l'emplacement physique de votre unité IP-Reach.

Appuyez sur <Ctrl+S> pour enregistrer les modifications ou sur <Echap> pour annuler les modifications et retourner au menu de configuration. Les modifications apportées à la configuration Radius n'entrent en vigueur qu'après le redémarrage d'IP-Reach.

Déconnexion des utilisateurs

Utilisez la touche <Tabulation>, <↑> ou <↓> pour sélectionner un utilisateur de l'écran Add, Change, or Delete User Accounts (Ajouter, modifier ou supprimer des comptes utilisateur) actuellement connecté à IP-Reach (**Logged in (Connecté) - YES (OUI)**) et appuyez sur la lettre <L> pour déconnecter l'utilisateur sélectionné. IP-Reach vous demande alors si vous souhaitez vraiment déconnecter l'utilisateur en question.

- **Y** : oui. L'utilisateur sélectionné est déconnecté d'IP-Reach et la session à distance prend fin. L'écran Add, Change, or Delete User Accounts (Ajouter, modifier ou supprimer des comptes utilisateur) d'IP-Reach, dans lequel tous les profils utilisateur sont répertoriés, s'affiche de nouveau. L'utilisateur sélectionné n'apparaît plus dans la liste des utilisateurs connectés.
- **N** : non. L'écran Add, Change, or Delete User Accounts (Ajouter, modifier ou supprimer des comptes utilisateur) d'IP-Reach, dans lequel tous les profils utilisateur sont répertoriés, s'affiche de nouveau. L'utilisateur sélectionné apparaît encore dans la liste des utilisateurs connectés.

Affichage de l'état d'IP-Reach

L'écran IP-Reach Event Log (Journal des événements d'IP-Reach) présente un fichier journal contenant des informations relatives aux ouvertures de session et aux activités de connexion d'IP-Reach. Le journal des événements regroupe les événements d'IP-Reach : connexion ou déconnexion des utilisateurs, échecs à la connexion, connexion et déconnexion des administrateurs au niveau de la console d'administration d'IP-Reach, modifications apportées par les administrateurs à la configuration du système, ajouts, modifications ou suppressions de profils utilisateur disposant de droits d'administrateur, activité du modem, démarrage et arrêt du système, erreurs survenues. L'heure et la date des différents événements sont également répertoriées. Pour connaître la liste des codes d'erreur ainsi que leur signification et la solution proposée, reportez-vous à l'**Annexe D : Guide de dépannage**. Un fichier journal peut contenir jusqu'à 2 048 événements.

IP-Reach procède également à une récupération automatique en cas d'erreur fatale. Lorsqu'une erreur fatale survient, elle est enregistrée et IP-Reach redémarre automatiquement. Lorsqu'une erreur de type autre qu'une erreur fatale survient, elle est enregistrée et IP-Reach attend que l'ensemble des utilisateurs se soit déconnecté du système pour redémarrer et veiller à ce que l'erreur qui était précédemment de type bénin ne devienne pas une erreur fatale.

```

IP-Reach v3.00b3      Name [IP-Reach]      IP Address [192.168.50.173]
Users [1]      Data In [0]s      Data Out [3653]s      Activity [kUma]_

Date      Time      Event
-----
12/12/2002 13:21:35 Anonymous timeout
12/12/2002 13:21:35 Anonymous disconnected
12/12/2002 19:13:39 Anonymous timeout
12/12/2002 19:13:39 Anonymous disconnected
12/13/2002 09:50:38 login failed 192.168.50.239
12/13/2002 09:50:40 ADMIN login failed 192.168.50.239
12/13/2002 09:50:42 ADMIN logged in from 192.168.50.239
12/13/2002 09:51:08 ADMIN disconnected
12/13/2002 10:57:18 System startup
12/13/2002 10:57:40 login failed 192.168.50.239
12/13/2002 10:57:43 ADMIN logged in from 192.168.50.239
12/13/2002 10:59:56 ADMIN logged out from the console
12/13/2002 11:01:31 ADMIN disconnected
12/13/2002 11:02:19 System startup
12/13/2002 11:03:28 ADMIN logged in from 192.168.50.239
<Bottom of the list>

ESC - Exit  C - Clear Log  N - Next page  P - Previous page  T - Top  B - Bottom

```

Redémarrage ou arrêt d'IP-Reach

Vous avez la possibilité de **redémarrer** <R> IP-Reach, d'**arrêter** <S> IP-Reach ou d'**annuler** <Echap> la commande de redémarrage ou d'arrêt. <R> Redémarre l'unité IP-Reach et rétablit l'écran d'initialisation d'IP-Reach sur la console d'administration d'IP-Reach.

Diagnostics

Lorsque vous naviguez dans le menu principal de la console d'administration, vous pouvez activer les fonctions de diagnostic d'IP-Reach à l'aide des touches <D> et <Entrée>.

Ces fonctions sont conçues pour permettre au support technique de Raritan de vous aider si vous rencontrez des problèmes avec votre unité IP-Reach. N'activez ces fonctions que si vous connaissez leur signification et leur utilisation recommandée. Si vous avez besoin de davantage d'informations, contactez le support technique de Raritan.

```

-[ IP-Reach Diagnostic Console ]-----[ 192.168.050.173 ]-
U      View log      LOG      Set log mask
<ENTER> View more log      M      Insert log marker
P      Pause Log      R      Resume log
C      Clear the log
NETSTATS Network Statistics      PING      Send a network ping
RESET      Reset to factory defaults      RESTART      Restarts IP-Reach

Type HELP <commandName> to get more information.
Type X to exit the diagnostic console.
>

```

Annexe A : Spécifications

ELEMENT	DIMENSIONS (LxPxH)	POIDS	TENSION
IPR-TR361	Boîtier de montage en rack 2U de 19" : 482 mm (L) x 540 mm (P) x 89 mm (H) 19" (L) x 21,25" (P) x 3,5" (H)	12,79 kg (28,2 lbs.)	Commutation automatique 110/220 V (Europe : 50/60 Hz)
IPR-TR362	Boîtier de montage en rack 2U de 19" : 482 mm (L) x 540 mm (P) x 89 mm (H) 19" (L) x 21,25" (P) x 3,5" (H)	12,97 kg (28,6 lbs.)	Commutation automatique 110/220 V (Europe : 50/60 Hz)
IPR-TR364	Boîtier de montage en rack 2U de 19" : 482 mm (L) x 540 mm (P) x 89 mm (H) 19" (L) x 21,25" (P) x 3,5" (H)	13,34 kg (29,4 lbs.)	Commutation automatique 110/220 V (Europe : 50/60 Hz)
IPR-M1	Boîtier de montage en rack 1U de 19" : 431 mm (L) x 264 mm (P) x 44 mm (H) 17" (L) x 10,4" (P) x 1,75" (H)	3,8 kg (8,4 lbs.)	Commutation automatique 110/220 V (Europe : 50/60 Hz)
IPR-M2	Boîtier de montage en rack 1U de 19" : 431 mm (L) x 264 mm (P) x 44 mm (H) 17" (L) x 10,4" (P) x 1,75" (H)	3,9 kg (8,6 lbs.)	Commutation automatique 110/220 V (Europe : 50/60 Hz)

Connexion à distance

Réseau : Ethernet 10BASE-T, 100BASE-TX
 Modem : modem 56K inclus (TR Series), port modem dédié (M Series)
 Protocoles : TCP/IP, UDP, SNMP

Logiciel Raritan Remote Client (RRC)

Système d'exploitation requis : Windows XP/NT/ME/2000

Entrée KVM

Clavier : PS/2

Souris : PS/2

Vidéo : VGA

Résolutions prises en charge :

Modes texte

640 x 480 à 60 Hz	1024 x 768 à 60 Hz
640 x 480 à 72 Hz	1024 x 768 à 70 Hz
640 x 480 à 75 Hz	1024 x 768 à 75 Hz
640 x 480 à 85 Hz	1024 x 768 à 85 Hz
800 x 600 à 56 Hz	1152 x 864 à 60 Hz
800 x 600 à 60 Hz	1152 x 864 à 75 Hz
800 x 600 à 72 Hz	1280 x 1024 à 60 Hz
800 x 600 à 75 Hz	
800 x 600 à 85 Hz	

Spécifications de câblage

Câble téléphonique RJ11 standard permettant de relier le modem à une ligne téléphonique (fourni)**

Câble UTP de catégorie 5 permettant la connexion au réseau

**Modèles TR Series uniquement

Spécifications des switch KVM

Prend en charge les switch KVM qui utilisent une interface utilisateur à l'écran (gammes de produits Paragon, Z-Series, MasterConsole MX⁴ et MasterConsole II de Raritan incluses).

Spécifications de sortie

Console d'accès locale : clavier PS/2, souris PS/2, vidéo HD15

Console d'administration locale : clavier PS/2, vidéo HD15

Annexe B : Fonctions SNMP

IP-Reach dispose d'un agent SNMP avec prise en charge MIB2 standard qui permet de contrôler facilement les systèmes de gestion réseau standard, tels que les solutions logicielles HP OpenView ou IBM Tivoli. IP-Reach répond aux requêtes d'obtention SNMP à l'aide de variables MIB2 standard. Cependant, pour des raisons de sécurité, seul un sous-ensemble de variables est fourni.

Annexe C : Foire Aux Questions

QUESTION	REPONSE
Qu'est-ce que IP-Reach ?	IP-Reach représente la plus simple, la plus rapide et la plus fiable des méthodes pour bénéficier de fonctions d'accès et de gestion sur plusieurs serveurs connectés à un switch KVM de Raritan - où que vous vous trouviez, et où que soient installés vos serveurs.
Comment IP-Reach fonctionne-t-il ?	IP-Reach se connecte aux ports clavier, vidéo et souris d'un serveur ou d'un switch KVM. Grâce à la puissante technologie de capture d'image et de compression de Raritan, il capture, numérise et compresse le signal vidéo avant de le transmettre à un ordinateur distant.
De quel niveau de contrôle dispose un utilisateur d'IP-Reach sur les serveurs cible connectés ?	L'utilisateur distant dispose d'un accès direct et d'un contrôle total des serveurs cible aux fins des opérations de maintenance, d'administration et de dépannage - de l'exécution d'applications via l'interface utilisateur aux interventions de niveau BIOS - et même de redémarrage.
Des logiciels d'accès à distance sont disponibles depuis longtemps. En quoi le système IP-Reach est-il différent ?	Avec IP-Reach, le logiciel IP-Reach s'exécute uniquement sur l'unité IP-Reach elle-même, et non sur chacun des serveurs cible. Les solutions logicielles d'accès à distance conventionnelles nécessitent le chargement et l'exécution de logiciels sur chacun des serveurs cible, qui doit dès lors disposer d'un système d'exploitation compatible. Cette situation peut créer des problèmes de compatibilité, de performances et de fiabilité sur les serveurs critiques.
Quelles sont les méthodes de connexion par accès distant utilisées par le dispositif IP-Reach ?	IP-Reach permet aux administrateurs réseau de choisir entre un accès distant via Internet, via un réseau local/étendu ou via un modem de connexion à distance. Cela signifie que les serveurs sont accessibles aussi bien sur la bande qu'en dehors de celle-ci et par conséquent, l'accès distant aux serveurs cible vitaux est toujours possible - même si le réseau n'est pas opérationnel.
Quels types d'ordinateurs IP-Reach peut-il contrôler à distance ?	IP-Reach fonctionne indépendamment de la configuration matérielle, du système d'exploitation ou du logiciel d'application du serveur cible pour accéder aux principaux dispositifs d'entrée/sortie du serveur cible - clavier, vidéo et souris mouse. Par conséquent, tout équipement compatible avec les interfaces clavier PC standard, les interfaces souris PC standard et les interfaces vidéo PC standard (VGA) peut être utilisé avec IP-Reach.
Un logiciel spécial est-il requis pour l'ordinateur distant ?	Chaque IP-Reach est fourni avec une copie du logiciel de contrôle IP-Reach. Ce logiciel d'accès distant s'exécute sur tous les ordinateurs distants équipés d'un système d'exploitation Windows 98 ou ultérieur et communique avec le logiciel IP-Reach installé sur l'unité IP-Reach via Internet, un réseau local ou étendu ou un modem d'appel à distance. Une fois le logiciel de contrôle IP-Reach installé, l'ordinateur distant se comporte de façon similaire à toute autre console utilisateur dans votre configuration KVM mais peut être situé n'importe où - dans la pièce à côté ou à l'autre bout du monde.
Quels sont les switch KVM de Raritan fonctionnant avec IP-Reach ?	IP-Reach prend actuellement en charge l'utilisation de l'ensemble des switch KVM de Raritan équipés d'un affichage à l'écran : Paragon, MasterConsole MX ⁴ et MasterConsole II.
Les autres marques de switch KVM fonctionnent-elles avec IP-Reach ?	Rien ne complémente mieux IP-Reach qu'un switch KVM de Raritan - particulièrement Paragon. En théorie toutefois, IP-Reach peut être utilisé avec tout switch KVM disposant d'un menu d'interface utilisateur à l'écran permettant d'accéder aux fonctions de commutation.
Puis-je continuer à accéder à ma configuration KVM localement ?	Oui. IP-Reach dispose d'un port connexion analogique utilisateur spécial offrant un accès direct à la configuration KVM. Ce port de communication propose un point d'accès local supplémentaire, ce qui est particulièrement important pour les switch à utilisateur unique ou pour disposer d'un accès critique aux serveurs lorsque le réseau est en panne.
IP-Reach peut-il être utilisé sans switch KVM ?	Oui. IP-Reach permet d'accéder directement à différents ordinateurs en se connectant aux ports clavier, vidéo et souris d'un ordinateur indépendant. Toutefois, ses aspects pratiques et sa valeur sont optimisés par l'utilisation d'un switch KVM.

QUESTION	REPOSE
IP-Reach est-il simple à installer ?	IP-Reach est très simple à installer. Il vous suffit de le connecter à un port utilisateur sur une configuration KVM existante et d'attribuer une adresse IP et/ou un numéro de téléphone pour les accès par modem.
Comment IP-Reach est-il administré ?	Les administrateurs accèdent à IP-Reach par l'intermédiaire d'une console d'administration d'IP-Reach connectée. Une interface de menus gérée depuis un simple clavier offre un accès direct aux options de configuration et de contrôle d'IP-Reach. Les profils utilisateur, paramètres de sécurité, options de configuration et diagnostics représentent quelques-unes seulement des options disponibles. La console d'administration d'IP-Reach peut être retirée de la salle de serveurs une fois la configuration initiale d'IP-Reach terminée. Par la suite, les configurations peuvent être définies à distance, via un navigateur Web.
Existe-t-il des fonctions de sécurité permettant de protéger mes serveurs cible d'une connexion à distance non autorisée ?	Oui. IP-Reach offre de nombreuses couches de sécurité. IP-Reach peut être configuré de façon à fournir une authentification de connexion et des transferts de données vidéo dotés d'un niveau de sécurité élevé au cours d'une session distante. Noms d'utilisateur, mots de passe, clés privées et chiffrement Secure Socket Layer (SSL) 128 bits sont tous disponibles. IP-Reach peut également fonctionner en tant que client RADIUS. En outre, tous les switch KVM de Raritan équipés d'une interface utilisateur à l'écran sont dotés d'un modèle de sécurité intégral, nécessitant la saisie d'un nom d'utilisateur et d'un mot de passe définis par l'administrateur lors d'accès aux serveurs.
Est-il possible de personnaliser IP-Reach pour optimiser les performances spécifiques à ma configuration KVM ?	Oui. Différentes procédures d'ajustement précis de la configuration sont disponibles. Le calibrage automatique des couleurs, le réglage de l'affichage à l'écran du KVM et l'ajustement des pointeurs de souris de la cible contribuent tous à optimiser les performances du système IP-Reach.
Est-il possible de personnaliser IP-Reach afin d'optimiser les performances du système en fonction de différentes méthodes et situations d'accès ?	Oui. IP-Reach propose différentes méthodes d'amélioration des performances, vous permettant d'optimiser la méthode de connexion de votre choix. Color Depth (Profondeur de couleur), Progressive Update (Mise à jour progressive) et Internet Flow Control (Contrôle du flux Internet) sont quelques-unes des options de réglage disponibles permettant de réduire les temps de réaction. L'option Color Depth (Profondeur de couleur), par exemple, peut même être réglée sur noir et blanc afin de réduire la charge des données au cours d'une connexion modem d'urgence de nuit avec des serveurs critiques par l'intermédiaire d'un réseau à bas débit.
Est-il possible d'utiliser IP-Reach sur un réseau VPN ?	Oui. Oui, IP-Reach est adaptable sur la plupart des configurations réseau utilisant le protocole TCP/IP. Il suffit à l'administrateur réseau d'ajouter IP-Reach en tant que noeud sur le réseau par l'intermédiaire de la console d'administration d'IP-Reach.
Quelle est la connexion la plus lente pouvant être gérée par IP-Reach ?	IP-Reach offre des performances évolutives reposant sur la bande passante disponible, jusqu'à 20 kbps.
Est-il possible d'établir une connexion avec IP-Reach par le biais d'un modem d'accès à distance sur une ligne PBX ?	Non. Les modems nécessitent une ligne téléphonique analogique.
Est-il possible d'utiliser IP-Reach au sein de mon réseau local ?	IP-Reach peut être utilisé dans tous les réseaux informatiques qui prennent en charge le protocole TCP/IP.
Quand IP-Reach utilise-t-il le protocole TCP ? le protocole UDP ?	IP-Reach utilise à la fois le protocole TCP et le protocole UDP. Le protocole TCP est cependant obligatoire alors que le protocole UDP est facultatif. Le protocole UDP est uniquement utilisé dans le cadre de la fonction IP-Reach de détection automatique (« navigation ») des unités IP-Reach dans un sous-réseau (reportez-vous au Chapitre 3 : Raritan Remote Client, Navigateur RRC). Si vous n'utilisez pas la fonction de navigation (et donc, par extension, le protocole DHCP), IP-Reach procédera aux communications à l'aide du protocole TCP uniquement.

Annexe D : Guide de dépannage

Problèmes et solutions proposées

PROBLEMES RELATIFS A LA CONNEXION A DISTANCE	SOLUTION
Je ne parviens pas à me connecter à IP-Reach via un modem d'accès à distance.	Assurez-vous que le modem sélectionné dans le champ correspondant de la fenêtre Add Connection (Ajouter une connexion) (connexion de type accès à distance) est le modem de votre ordinateur distant. Il est possible que les connexions multiples soient activées (globalement ou individuellement), le modem d'IP-Reach n'autorise cependant qu'une seule connexion à distance à la fois. Assurez-vous que personne n'est connecté via le modem. Assurez-vous que votre profil utilisateur autorise l'accès par l'intermédiaire d'un modem et qu'IP-Reach est configuré de manière à autoriser une interface modem (écran Network Configuration (Configuration réseau)). Assurez-vous que le port de communication sélectionné par l'administration réseau au niveau de l'écran Network Configuration (Configuration réseau) correspond au port défini dans votre profil de connexion.
Je ne parviens pas à me connecter à IP-Reach via le réseau local/étendu ou Internet.	Vérifiez de nouveau les paramètres IP définis pour IP-Reach au niveau de la console d'administration d'IP-Reach ou de la fenêtre de la Admin Console (Console d'administration) distante. Accédez à l'écran Network Configuration (Configuration réseau) et assurez-vous que les adresses IP définies pour les paramètres relatifs à l'adresse IP, au masque de sous-réseau et à la passerelle par défaut sont toujours correctes et conformes aux instructions de votre administrateur réseau. Assurez-vous que votre profil utilisateur autorise l'accès réseau et qu'IP-Reach est configuré de manière à autoriser une interface réseau. Assurez-vous que le port de communication sélectionné par l'administration réseau au niveau de l'écran Network Configuration (Configuration réseau) correspond au port défini dans votre profil de connexion. Assurez-vous que la configuration réseau est correcte en envoyant une commande PING de l'ordinateur distant vers IP-Reach.
Je ne parviens pas à me connecter à IP-Reach via un navigateur Web.	Vérifiez de nouveau les paramètres IP définis pour IP-Reach au niveau de la console d'administration d'IP-Reach ou de la fenêtre de la Admin Console (Console d'administration) distante. Accédez à l'écran Network Configuration (Configuration réseau) et assurez-vous que les adresses IP définies pour les paramètres relatifs à l'adresse IP, au masque de sous-réseau et à la passerelle par défaut sont toujours correctes et conformes aux instructions de votre administrateur réseau. Assurez-vous que votre profil utilisateur autorise l'accès par l'intermédiaire d'un navigateur Web et qu'IP-Reach est configuré de manière à autoriser les navigateurs Web.
Je ne parviens pas à me connecter à IP-Reach et l'affichage semble bloqué sur la fenêtre Login (Connexion) .	Assurez-vous que vous utilisez un nom d'utilisateur et un mot de passe corrects et valables. Assurez-vous que vous saisissez le nom d'utilisateur et le mot de passe en utilisant la même association de majuscules et de minuscules que lors de leur création. Faites glisser la fenêtre Login (Connexion) sur le côté et affichez la fenêtre Connection Status (Etat de la connexion), située en arrière-plan. La fenêtre Connection Status (Etat de la connexion) contient l'ensemble des détails relatifs à vos tentatives de connexion et offre parfois des explications spécifiques au problème rencontré.

PROBLEMES RELATIFS A LA CONSOLE UTILISATEUR ANALOGIQUE DIRECTE	SOLUTION
La console utilisateur analogique directe ne fonctionne pas.	Assurez-vous que le switch KVM fonctionne correctement. Assurez-vous qu'IP-Reach est sous tension. IP-Reach doit être sous tension pour que la console utilisateur analogique directe fonctionne. Il est possible que le câble situé à l'intérieur d'IP-Reach et utilisé pour la connexion avec le ou les ports de la console utilisateur analogique directe soit déconnecté. Contactez le support technique de Raritan pour obtenir de l'aide.
La console utilisateur analogique directe ne me permet pas d'obtenir un contrôle clavier/souris stable au niveau du serveur cible actif.	Le contrôle clavier/souris d'un serveur cible actif à l'aide d'une console utilisateur analogique directe est partagé entre les différents utilisateurs distants actuellement connectés, en fonction de la première saisie clavier/souris active. Assurez-vous qu'aucun des utilisateurs distants n'essaie de contrôler le serveur cible actif.
Je ne parviens pas à localiser le serveur cible que je recherche sur la console utilisateur analogique directe.	Assurez-vous que vous procédez à la recherche sur la console utilisateur analogique directe connectée au port utilisateur correct. Rappelez-vous, il est possible de relier les consoles utilisateur analogiques directes aux ports 1 à 4. Chaque console utilisateur affiche le chemin du port KVM correspondant. La console utilisateur relié au port utilisateur 1, par exemple, affiche le chemin KVM relié au port KVM 1. De même, la console utilisateur relié au port utilisateur 2 affiche le chemin KVM relié au port KVM 2, etc.

PROBLEMES RELATIFS AU CLAVIER	SOLUTION
IP-Reach refuse les commandes de clavier émises par l'ordinateur distant.	La fenêtre permettant un contrôle clavier correct est la fenêtre IP-Reach du logiciel de contrôle IP-Reach. Assurez-vous que la fenêtre dans laquelle vous effectuez la saisie est active. Effacez les signaux de clavier afin de vous assurer que le signal de relâchement ou de coupure a été reçu - procédez à plusieurs appuis répétés sur les touches <Ctrl>, <Maj> et <Tabulation> de votre clavier. Assurez-vous que l'utilisateur distant dispose de droits par rapport au clavier et à la souris. Fermez et redémarrez le logiciel IP-Reach.
J'ai appuyé sur la touche Verr. maj. sur mon ordinateur distant. Le repère CAPS apparaît dans la barre d'état d'IP-Reach mais le voyant de verrouillage des majuscules du clavier de mon ordinateur distant ne s'allume pas.	Ceci est normal. Utilisez les indicateurs de la barre d'état pour déterminer l'état des touches CAPS au niveau du serveur cible. Si un utilisateur local a modifié, au niveau du clavier de la console utilisateur analogique directe, un des états de verrouillage des touches (Verr. maj., Verr num ou Arrêt défil) du serveur cible, il est alors possible que l'état du serveur ne corresponde pas à celui du clavier de l'ordinateur distant.
Le clavier ne fonctionne pas et le témoin vert d'au moins un des ports KVM, situé sur la partie arrière d'IP-Reach, ne clignote pas mais reste allumé en permanence.	Réinitialisez les puces du clavier d'IP-Reach en procédant à une remise sous tension. Veillez à mettre IP-Reach et l'ensemble des switch KVM connectés hors tension, faute de quoi les puces KVM d'IP-Reach utiliseront les switch KVM comme source d'énergie et ne seront pas réinitialisées.
J'accède à IP-Reach via un navigateur Web et le clavier ne fonctionne pas. Rien ne se produit lors de la saisie.	Cliquez dans la barre de titre de la fenêtre, sous la barre d'outils d'IP-Reach, pour activer l'affichage de la fenêtre. Le clavier ne fonctionne pas lorsque la fenêtre affichée n'est pas la fenêtre active.

PROBLEMES RELATIFS A L'INTERFACE UTILISATEUR A L'ECRAN KVM	SOLUTION
L'interface utilisateur à l'écran du switch KVM connecté ne s'affiche pas lorsque je clique sur le bouton Enter On-Screen Menu (Accéder au menu à l'écran) . Rien ne se produit.	Il est possible qu'IP-Reach ne soit pas configuré sur l'activateur de raccourci-clavier adapté au switch KVM. Le raccourci-clavier défini par défaut dans la fenêtre Options d'IP-Reach est <Arrêt défil> ou Arrêt défil+Arrêt défil . Assurez-vous que le raccourci-clavier défini dans la fenêtre Options est similaire à celui qui commande l'interface utilisateur à l'écran du switch KVM de base connecté à IP-Reach. Dans le menu de la fenêtre IP-Reach , sélectionnez Tools (Outils) > Options . La fenêtre Options s'affiche alors. Sélectionnez le raccourci-clavier qui permet d'activer l'interface utilisateur à l'écran du switch KVM connecté. Arrêt défil+Arrêt défil = <Arrêt défil>, Verr num+Verr num = <Verr num> et Verr. maj.+Verr. maj. = <Verr. maj.>. Cliquez sur [OK] pour poursuivre.
Un switch KVM est connecté à mon ordinateur distant. Lorsque je saisis <Arrêt défil> <Arrêt défil> (ou un autre raccourci-clavier pour l'interface utilisateur à l'écran du switch KVM) sur le clavier de l'ordinateur distant, deux interfaces utilisateur à l'écran sont activées : une pour le switch KVM connecté à mon ordinateur distant et un autre pour le switch KVM de base connecté à IP-Reach.	Sur la console utilisateur de l'ordinateur distant, quittez l'interface utilisateur à l'écran du switch KVM correspondant à l'ordinateur distant en appuyant une fois sur la touche <Echap> . Patientez quelques secondes : l'interface utilisateur à l'écran du switch KVM correspondant à l'ordinateur distant disparaît. Pour éviter ce problème, réinitialisez le switch KVM connecté à l'ordinateur distant de manière à ce qu'il utilise un raccourci-clavier différent de celui du switch KVM de base connecté à IP-Reach. Vous pouvez également utiliser les commandes IP-Reach pour activer uniquement l'interface utilisateur à l'écran du switch KVM de base connecté à IP-Reach - appuyez sur la touche Enter On-Screen Menu (Accéder au menu à l'écran) .
La déconnexion du KVM lors de la déconnexion est activée dans l'écran Security Configuration (Configuration de la sécurité) . Pourtant, lorsque l'utilisateur distant se déconnecte, IP-Reach ne se déconnecte pas du KVM.	Assurez-vous que le raccourci-clavier défini dans la fenêtre Options est similaire à celui qui commande l'interface utilisateur à l'écran du switch KVM de base connecté à IP-Reach.

PROBLEMES RELATIFS A LA SOURIS	SOLUTIONS
Le pointeur de la souris du serveur cible est trop lent en comparaison du pointeur de la souris d'IP-Reach . Lors de l'activation d'un nouveau canal du serveur cible, la souris s'arrête et/ou n'est plus synchronisée.	Lorsque vous travaillez depuis un ordinateur distant, il existe un léger décalage entre le pointeur de la souris d'IP-Reach , plus grand, et le pointeur de la souris du serveur cible , plus petit. Ce décalage est le résultat normal de variations incontrôlables au niveau de la vitesse de la connexion distante (Internet, modem d'accès direct ou réseau). Lors de l'affichage des images vidéo, IP-Reach procède automatiquement à une resynchronisation et aligne les pointeurs des souris. Patientez quelques secondes après l'activation d'une nouvelle image vidéo, le temps que le recalibrage automatique ait lieu et que les deux pointeurs de souris s'alignent. Si vous ne souhaitez pas attendre la fin de cette opération de calibrage automatique ou si les deux pointeurs de souris ne sont toujours pas synchronisés, cliquez sur Synchroniser la souris ou appuyez simultanément sur les touches <Ctrl-Alt-S> . Le réalignement manuel des deux pointeurs a alors lieu.

PROBLEMES RELATIFS A LA SOURIS	SOLUTIONS
	Réglez le mouvement du pointeur de la souris du serveur cible. Pour les serveurs cible fonctionnant sous Windows 2000, réglez la vitesse de déplacement de la souris des serveurs cible sur le paramètre de vitesse moyenne, entre la vitesse rapide et la vitesse lente, et la vitesse d'accélération du mouvement de la souris des serveurs cible sur <Désactivé> ou <Aucune>. Pour les serveurs cible fonctionnant Windows 95, 98 ou NT, réglez la vitesse de déplacement de la souris des serveurs cible sur le paramètre le plus faible. Les paramètres de couleur ne sont pas calibrés de manière optimale. Procédez à un calibrage automatique des couleurs (Chapitre 3 : Raritan Remote Client, Calibrage des couleurs).
Le pointeur de la souris d'IP-Reach, plus grand, est trop lent ou n'est pas synchronisé (aligné) sur le pointeur de la souris du serveur cible, plus petit.	Cliquez sur Synchroniser la souris ou appuyez sur <Ctrl-Alt-S>. Assurez-vous que les serveurs cible utilisent un pilote de souris Windows standard. Pour les serveurs cible fonctionnant sous Windows 2000, réglez la vitesse de déplacement de la souris des serveurs cible sur le paramètre de vitesse moyenne, entre la vitesse rapide et la vitesse lente, et la vitesse d'accélération du mouvement de la souris des serveurs cible sur <Aucune>. Pour les serveurs cible fonctionnant Windows 95, 98 ou NT, réglez la vitesse de déplacement de la souris des serveurs cible sur le paramètre le plus faible possible. Cliquez sur Détection automatique des signaux vidéo ou appuyez simultanément sur les touches <Ctrl-Alt-A>.
IP-Reach refuse ma souris.	IP-Reach ne prend pas en charge les souris de type série ou les pilotes de souris non standard. Il prend uniquement en charge les souris de type PS/2 et les pilotes de souris Windows standard. Il est possible que les autres pilotes de souris fonctionnent avec IP-Reach. De nombreuses modifications sont néanmoins nécessaires au niveau des paramètres de la souris pour trouver un ensemble de paramètres de déplacement acceptables. Si vous devez utiliser un pilote de souris non pris en charge par IP-Reach sur un serveur cible, réglez l'accélération de la souris sur <Aucune> et la vitesse de la souris sur <Lente>.
Le pointeur de la souris d'IP-Reach, et le pointeur de la souris du serveur cible ne sont pas alignés dans certains écrans d'administration de Windows NT, tels que l'écran de connexion NT.	Les écrans de connexion ou d'administration de Windows NT peuvent rétablir les vitesses d'accélération/de déplacement par défaut du pointeur de la souris. Il est donc possible que la synchronisation de la souris ne soit pas optimale dans ces écrans. Si vous savez paramétrer le registre du serveur cible Windows NT, vous pouvez obtenir un alignement de la souris IP-Reach de meilleure qualité dans les écrans d'administration NT en accédant à l'éditeur de registre du serveur cible et en modifiant les paramètres suivants : vitesse par défaut du pointeur de la souris utilisateur = 0, seuil de la souris 1 = 0, seuil de la souris 2 = 0.

PROBLEMES RELATIFS AU SERVEUR CIBLE	SOLUTION
Lors du redémarrage d'un serveur cible depuis un ordinateur distant, via IP-Reach, je ne parviens pas à accéder au BIOS du serveur cible. Il semble qu'IP-Reach n'accepte pas la frappe de la commande de saisie BIOS.	Pour accéder au BIOS du serveur cible, commencez par désactiver temporairement la case à cocher Sense video mode changes automatically (Détection automatique des modifications du mode vidéo) de la fenêtre Video Settings (Paramètres vidéo) , à laquelle vous accédez à l'aide du bouton Paramètres vidéo de la barre d'outils d'IP-Reach. La détection automatique des paramètres vidéo ralentit l'affichage de la procédure de redémarrage et rend l'envoi de frappes d'accès au BIOS du serveur cible plus difficile pour l'ordinateur distant. En effet, la détection automatique exige un travail constant de la part d'IP-Reach en raison du changement rapide d'écrans vidéo au niveau du serveur cible lors du redémarrage. La désactivation des cases à cocher de détection automatique permet à IP-Reach d'accepter et de transmettre les frappes d'accès au BIOS. Il intervient également dans l'interprétation immédiate des changements rapides d'écrans vidéo. Une fois l'accès au BIOS réalisé, veillez à réactiver la case à cocher.

PROBLEMES RELATIFS A IP-REACH	SOLUTION
Aucune activité de contrôle ou de capture d'image n'a lieu. IP-Reach semble être verrouillé.	Il est possible qu'un câble interne de données série, qui relie la carte de capture d'image à la carte mère d'IP-Reach, soit déconnecté. Contactez le support technique de Raritan pour obtenir de l'aide.
Je ne parviens pas à mettre IP-Reach hors tension.	L'interrupteur d'alimentation principal de l'unité IP-Reach est situé sur la partie arrière de l'unité. Pour mettre IP-Reach hors tension, maintenez l'interrupteur enfoncé pendant quelques secondes. Pour remettre IP-Reach sous tension, appuyez de nouveau sur l'interrupteur.
Lors des coupures de courant, IP-Reach ne redémarre pas automatiquement une fois le courant rétabli.	Accédez au BIOS d'IP-Reach et assurez-vous que l'option « Power Lost Resume State » (Etat de reprise lors de coupures de courant) est réglée sur « Last State » (Dernier état). Une fois le courant rétabli, IP-Reach se remet SOUS tension uniquement s'il se trouvait SOUS tension lors de la coupure de courant.

PROBLEMES RELATIFS A LA VIDEO	SOLUTION
Lors de l'activation d'un nouveau canal du serveur cible, la vidéo n'est pas nette. Une bordure noire apparaît parfois sur le bord de l'écran du serveur cible.	Cliquez sur Détection automatique des signaux vidéo ou appuyez simultanément sur les touches <Ctrl-Alt-A>. IP-Reach procède alors aux réglages des paramètres vidéo. Si la vidéo ne s'améliore pas, il peut être nécessaire de régler manuellement les paramètres vidéo. Contactez le support technique de Raritan pour connaître les modifications à apporter à la fenêtre Video Settings (Paramètres vidéo). Assurez-vous que les serveurs cible disposent de temps de passage en blanc standard. Les temps de passages en blanc horizontaux et verticaux doivent être à peu près équivalents aux valeurs VESA standard.
Lors de l'affichage à distance d'un serveur cible, l'image vidéo présente des blocs mobiles de	Les paramètres de couleur de l'onglet Video Settings (Paramètres vidéo) de la fenêtre Video (Vidéo) ne sont pas définis correctement. Procédez à un réglage manuel jusqu'à ce que les

PROBLEMES RELATIFS A LA VIDEO	SOLUTION
couleurs incorrectes qui semblent suivre le déplacement du pointeur de la souris.	blocs de couleur disparaissent ou procédez à un calibrage automatique des couleurs (reportez-vous au Chapitre 3 : Raritan Remote Client, Calibrage des couleurs).
L'écran présente un certain nombre de petites erreurs visuelles ou de grains dont les couleurs manquent et qui doivent être supprimés.	Cliquez sur Actualiser l'écran dans la barre d'outils d'IP-Reach ou appuyez simultanément sur les touches <Ctrl-Alt-R>.
La vidéo semble bloquée en mode de détection automatique et le décompte du message de détection automatique, situé au centre de l'écran, est de plus en plus important.	Cliquez sur Détection automatique des signaux vidéo lors de la détection automatique pour interrompre l'opération. Vérifiez la résolution de votre serveur cible afin de vous assurer qu'elle est prise en charge par IP-Reach.

PROBLEMES RELATIFS AU NAVIGATEUR WEB	SOLUTION
Je ne parviens pas à me connecter à IP-Reach via un navigateur Web.	Vérifiez de nouveau les paramètres IP définis pour IP-Reach au niveau de la console d'administration d'IP-Reach ou de la fenêtre de la Admin Console (Console d'administration) distante. Accédez à l'écran Network Configuration (Configuration réseau) et assurez-vous que les adresses IP définies pour les paramètres relatifs à l'adresse IP, au masque de sous-réseau et à la passerelle par défaut sont toujours correctes et conformes aux instructions de votre administrateur réseau. Assurez-vous que votre profil utilisateur autorise l'accès par l'intermédiaire d'un navigateur Web et qu'IP-Reach est configuré de manière à autoriser les navigateurs Web.

Fichier du journal des événements et codes d'erreur à l'écran

Lorsqu'un problème survient, IP-Reach affiche ou enregistre un code d'erreur dans l'écran **IP-Reach Event Log (Journal des événements d'IP-Reach)**. Les codes d'erreur sont des nombres hexadécimaux composés de huit chiffres et de deux parties : les quatre premiers chiffres se rapportent au type d'erreur et les quatre derniers chiffres se rapportent à l'emplacement de l'erreur.

Les quatre derniers chiffres des codes d'erreur d'IP-Reach contribuent souvent à déterminer l'origine de l'anomalie du système. Vous trouverez ci-dessous une liste de codes d'emplacement (quatre derniers chiffres du code d'erreur) ainsi que leur signification.

CODE D'ERREUR (QUATRE DERNIERS CHIFFRES)	SIGNIFICATION	RECOMMANDATION
0001 - 0003	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0004	Impossible de lire le fichier de configuration lors du démarrage. Il est possible que le fichier soit corrompu, le système de fichiers soit endommagé ou que le fichier de configuration soit issu d'une ancienne version d'IP-Reach.	Saisissez de nouveau les informations relatives à la configuration et procédez au redémarrage. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0005	Le fichier de configuration ne peut être localisé. Il est possible qu'il s'agisse du premier démarrage d'IP-Reach ou que le système de fichiers soit corrompu.	Saisissez de nouveau les informations relatives à la configuration et procédez au redémarrage. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0006	Le fichier de configuration ne peut être enregistré. Il est possible que le système de fichiers soit corrompu ou que le disque dur ne réponde pas.	Réessayez. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0007 - 0008	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
Supprimer	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0009	Impossible de localiser la carte de capture d'image	Mettez le système hors tension et assurez-vous que la carte de capture d'image est bien insérée. Si le problème persiste, il est possible que le matériel de votre unité IP-Reach présente une anomalie.

CODE D'ERREUR (QUATRE DERNIERS CHIFFRES)	SIGNIFICATION	RECOMMANDATION
000A	La carte de capture d'image ne répond pas correctement.	Mettez le système hors tension et assurez-vous que la carte de capture d'image est bien insérée. Si le problème persiste, il est possible que le matériel de votre unité IP-Reach présente une anomalie.
000B	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
000C - 000F	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0011	Impossible de localiser le contrôleur Ethernet	Le matériel de votre unité IP-Reach présente une anomalie.
0012	Impossible de localiser le modem	Mettez le système hors tension et assurez-vous que la carte de capture d'image est bien insérée. Si le problème persiste, il est possible que le matériel de votre unité IP-Reach présente une anomalie.
0013	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0014	L'adresse IP présente une anomalie.	Vérifiez la configuration de l'adresse IP et procédez au redémarrage.
0015	Le serveur DHCP ne répond pas. IP-Reach ne peut obtenir une adresse IP.	Assurez-vous que votre serveur DHCP fonctionne correctement et redémarrez IP-Reach.
0016 - 0019	Un des fichiers de démarrage d'IP-Reach présente une anomalie.	Réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
001A	Une erreur s'est produite lors de l'initialisation du point de connexion UDP.	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
001B	Une erreur s'est produite lors de l'initialisation du point de connexion en écriture TCP.	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
001C	Une erreur s'est produite lors de l'initialisation du point de connexion en lecture TCP.	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
001D - 001E	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.

CODE D'ERREUR (QUATRE DERNIERS CHIFFRES)	SIGNIFICATION	RECOMMANDATION
001F	Impossible d'écouter le point de connexion en écriture TCP	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0020	Impossible d'écouter le point de connexion en lecture TCP	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0021	Echec de la procédure d'écoute TCP	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0022	Echec de la procédure d'écoute UDP	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0023	Echec de l'écriture SSL	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0024	Echec de la lecture SSL	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0025	Erreur d'allocation mémoire	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0026 - 0029	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
002A - 002F	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
0030-0039	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.
003A - 003F	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.

CODE D'ERREUR (QUATRE DERNIERS CHIFFRES)	SIGNIFICATION	RECOMMANDATION
0040	Erreur d'allocation ressources	Redémarrez IP-Reach. Assurez-vous que le test de mémoire BIOS localise au moins 64 Mo de mémoire vive. Si le problème persiste, réinstallez le logiciel et le système de fichiers à l'aide du CD-ROM de récupération.